

UNIVERSIDADE FEDERAL DO PARANÁ

MATHEUS FALK

PROTEÇÃO DE DADOS PESSOAIS E A DEMOCRACIA:
A “DECISÃO DE ADEQUAÇÃO” BRASILEIRA COMO RESPOSTA AO
COLONIALISMO DE DADOS

CURITIBA

2024

MATHEUS FALK

PROTEÇÃO DE DADOS PESSOAIS E A DEMOCRACIA:
A “DECISÃO DE ADEQUAÇÃO” BRASILEIRA COMO RESPOSTA AO
COLONIALISMO DE DADOS

Tese apresentada ao Programa de Pós-Graduação em Direito, no Setor de Ciências Jurídicas, na Universidade Federal do Paraná, como requisito parcial à obtenção do grau de Doutor em Direito.

Orientador: Prof. Dr. Cesar Antonio Serbena

CURITIBA

2024

DADOS INTERNACIONAIS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP)
UNIVERSIDADE FEDERAL DO PARANÁ
SISTEMA DE BIBLIOTECAS – BIBLIOTECA DE CIÊNCIAS JURÍDICAS

Falk, Matheus

Proteção de dados pessoais e a democracia: a "decisão de adequação" brasileira como resposta ao colonialismo de dados / Matheus Falk. – Curitiba, 2024.
1 recurso on-line : PDF.

Tese (Doutorado) – Universidade Federal do Paraná,
Setor de Ciências Jurídicas, Programa de Pós-graduação
em Direito.

Orientador: Cesar Antonio Serbena.

1. Proteção de dados. 2. Brasil. [Lei geral de proteção
de dados pessoais (2018)]. I. Serbena, Cesar Antonio.
II. Título. III. Universidade Federal do Paraná.

Bibliotecário: Pedro Paulo Aquilante Junior – CRB-9/1626



MINISTÉRIO DA EDUCAÇÃO
SETOR DE CIÊNCIAS JURÍDICAS
UNIVERSIDADE FEDERAL DO PARANÁ
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO DIREITO -
40001016017P3

ATA Nº525

ATA DE SESSÃO PÚBLICA DE DEFESA DE DOUTORADO PARA A OBTENÇÃO DO GRAU DE DOUTOR EM DIREITO

No dia vinte e oito de novembro de dois mil e vinte e quatro às 09:00 horas, na sala de Defesas - 317 - 3º andar, PPGD UFPR - Prédio Histórico da UFPR - Praça Santos Andrade, 50, foram instaladas as atividades pertinentes ao rito de defesa de tese do doutorando **MATHEUS FALK**, intitulada: **PROTEÇÃO DE DADOS PESSOAIS E A DEMOCRACIA: A decisão de adequação brasileira como resposta ao colonialismo de dados**, sob orientação do Prof. Dr. CÉSAR ANTONIO SERBENA. A Banca Examinadora, designada pelo Colegiado do Programa de Pós-Graduação DIREITO da Universidade Federal do Paraná, foi constituída pelos seguintes Membros: CÉSAR ANTONIO SERBENA (UNIVERSIDADE FEDERAL DO PARANÁ), ALINE MACOHIN (SERPRO), EDNA TORRES FELÍCIO (CENTRO UNIVERSITARIO DE PINHAIS), FERNANDO ANDREONI VASCONCELLOS (ESCOLA DA MAGISTRATURA DO PARANÁ). A presidência iniciou os ritos definidos pelo Colegiado do Programa e, após exarados os pareceres dos membros do comitê examinador e da respectiva contra argumentação, ocorreu a leitura do parecer final da banca examinadora, que decidiu pela APROVAÇÃO. Este resultado deverá ser homologado pelo Colegiado do programa, mediante o atendimento de todas as indicações e correções solicitadas pela banca dentro dos prazos regimentais definidos pelo programa. A outorga de título de doutor está condicionada ao atendimento de todos os requisitos e prazos determinados no regimento do Programa de Pós-Graduação. Nada mais havendo a tratar a presidência deu por encerrada a sessão, da qual eu, CÉSAR ANTONIO SERBENA, lavrei a presente ata, que vai assinada por mim e pelos demais membros da Comissão Examinadora.

CURITIBA, 28 de Novembro de 2024.

CÉSAR ANTONIO SERBENA
Presidente da Banca Examinadora

ALINE MACOHIN
Avaliador Externo (SERPRO)

EDNA TORRES FELÍCIO
Avaliador Externo (CENTRO UNIVERSITARIO DE PINHAIS)

FERNANDO ANDREONI VASCONCELLOS
Avaliador Externo (ESCOLA DA MAGISTRATURA DO PARANÁ)



MINISTÉRIO DA EDUCAÇÃO
SETOR DE CIÊNCIAS JURÍDICAS
UNIVERSIDADE FEDERAL DO PARANÁ
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO DIREITO -
40001016017P3

TERMO DE APROVAÇÃO

Os membros da Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação DIREITO da Universidade Federal do Paraná foram convocados para realizar a arguição da tese de Doutorado de **MATHEUS FALK** intitulada: **PROTEÇÃO DE DADOS PESSOAIS E A DEMOCRACIA: A decisão de adequação brasileira como resposta ao colonialismo de dados**, sob orientação do Prof. Dr. CÉSAR ANTONIO SERBENA, que após terem inquirido o aluno e realizada a avaliação do trabalho, são de parecer pela sua APROVAÇÃO no rito de defesa.

A outorga do título de doutor está sujeita à homologação pelo colegiado, ao atendimento de todas as indicações e correções solicitadas pela banca e ao pleno atendimento das demandas regimentais do Programa de Pós-Graduação.

CURITIBA, 28 de Novembro de 2024.

CÉSAR ANTONIO SERBENA
Presidente da Banca Examinadora

EDNA TORRES FELÍCIO
Avaliador Externo (CENTRO UNIVERSITARIO DE PINHAIS)

ALINE MACOHIN
Avaliador Externo (SERPRO)

FERNANDO ANDREONI VASCONCELLOS
Avaliador Externo (ESCOLA DA MAGISTRATURA DO PARANÁ)

*A José Luís, Berenice, Gabriel e Amanda,
que ocupam para sempre um lugar especial
em meu coração.*

*Com profunda gratidão por cada gesto de
amor, carinho, apoio e companheirismo.*

AGRADECIMENTOS

Agradeço aos meus pais, José Luís e Berenice, pelo amor incondicional, pela paciência infinita e por terem sido sempre meu porto seguro. Vocês acreditaram em mim até quando eu duvidava. Cada conquista minha carrega a força da dedicação e dos valores que vocês me ensinaram. Obrigado por terem me incentivado, apoiado e amado durante toda minha vida.

Ao meu irmão, Gabriel, agradeço por ser meu amigo e meu exemplo de coragem e determinação. Obrigado por me acolher sempre e por me inspirar com sua independência, retidão e determinação, qualidades que admiro profundamente.

Agradeço aos meus avós, *in memoriam*, Carlos e Maria Eva, Pedro e Lucíola, e Rosa Maria, cujo amor e carinho deixaram marcas profundas em minha vida. Vocês me ensinaram valores que carrego com orgulho, e a força de nossa ancestralidade me guia e inspira diariamente.

À Rene, Eliane e Anísia, que me acolheram como parte de sua família, oferecendo carinho, apoio e entendimento inestimáveis ao longo desta jornada. Agradeço pelo incentivo e compreensão durante todo esse período.

Aos amigos que marcaram minha caminhada, novos e de longa data, tanto em Curitiba quanto em União da Vitória, minha eterna gratidão. Vocês foram meu suporte em muitos momentos difíceis e compartilharam comigo as alegrias e conquistas que fizeram esta jornada valer a pena. Obrigado pela presença e palavras de incentivo e, acima de tudo, pela amizade verdadeira, que sempre me impulsionou a seguir em frente.

À Universidade Federal do Paraná (UFPR), especialmente à sua ilustre Faculdade de Direito, que foi minha casa por mais de dez anos. Este espaço, que guarda tanta história e excelência, me proporcionou uma educação de qualidade, não apenas na formação acadêmica, mas também no desenvolvimento humano. Foi ali que aprendi a pensar criticamente, a valorizar a justiça e a me moldar como cidadão consciente. A UFPR foi fundamental em cada passo desta trajetória, e levarei comigo a lembrança de aulas, debates e experiências vividas nessas salas e corredores.

Ao meu orientador, Cesar Antonio Serbena, expresso minha mais profunda gratidão. Obrigado por acreditar em mim. Sua paciência, confiança e sabedoria foram

fundamentais para a realização deste trabalho. Obrigado por ser uma inspiração e por me guiar com tanto empenho e dedicação.

À Universidade Estadual do Paraná, *campus* de União da Vitória, agradeço por me acolher como docente e se tornar, desde então, minha nova casa. É sob esse teto que me alio à luta por uma educação pública, gratuita e de qualidade, unindo esforços com seu corpo docente, discente e técnico, a quem dedico minha mais sincera gratidão.

Ao Programa de Excelência Acadêmica (PROEX) da CAPES, agradeço pelo apoio financeiro que tornou possível a realização desta pesquisa. Sem o suporte da bolsa de doutorado, este sonho não teria se realizado.

À educação pública brasileira, agradeço por ser o alicerce de transformação social e de esperança em um país que ainda luta por justiça e igualdade. Que essa educação continue sendo a luz que guia futuros sonhadores como eu.

Por fim, à Amanda, minha companheira de vida e de luta. Esta conquista é nossa, porque sem o seu amor, paciência e força, as linhas desta tese, ainda que escritas, não teriam significado. É em você que encontro o sentido de tudo, o abrigo nas tempestades e a alegria das pequenas vitórias. Cada palavra aqui também carrega um pedaço seu, porque você sempre esteve comigo, acreditando quando eu duvidava e me incentivando a seguir em frente, mostrando que tudo valeria a pena. Obrigado por ser o coração que pulsa em cada página deste sonho realizado.

A cada pessoa mencionada – e também àquelas que ficaram nas entrelinhas deste texto – deixo meu coração repleto de gratidão.

Fell the breeze?

Time's so near you can almost taste the freedom

There's a warm wind from the south

Hoist the sail and we'll be gone

By morning, this will all seem like a dream

And if I don't return to sing the song, maybe just as well

I've seen the news and there's not much I can do...alone

Is there anybody listening?

Is there anyone who smiles without a mask?

What's behind the words-images

They know will please us?

I'll take what's real (bring up the lights)

Is there anybody listening?

Is there anyone that sees what's going on?

Read between the lines

Criticize the words they're selling

Think for yourself and feel the walls

Become sand beneath your feet

Queensrÿche – *Anybody Listening?*

Por eso, muchacho, no partas ahora

Soñando el regreso

Que el amor es simple

Y a las cosas simples las devora el tiempo

Mercedes Sosa – *Canción De Las Simples Cosas*

Porque se chamavam homens

Também se chamavam sonhos

E sonhos não envelhecem...

Milton Nascimento – *Clube da Esquina nº 2*

RESUMO

Este trabalho tem como objetivo aprofundar o estudo sobre o direito à proteção de dados pessoais no Brasil, com foco na transferência internacional de dados e no papel da Autoridade Nacional de Proteção de Dados (ANPD) na emissão de "decisões de adequação". A pesquisa propõe uma análise crítica sobre a regulação dessa matéria, com especial atenção à Resolução CD/ANPD nº 19/2024, que regulamenta a transferência internacional de dados pessoais no Brasil, conforme previsto na Lei Geral de Proteção de Dados (LGPD). A tese defende que a ANPD não apenas possui a faculdade, mas o dever de emitir tais decisões, a fim de assegurar que os dados pessoais de brasileiros sejam protegidos adequadamente ao serem transferidos para países com legislações diferentes, evitando que esses dados sejam tratados de forma incompatível com os padrões brasileiros. A pesquisa se estrutura em três capítulos. O primeiro explora a interseção entre democracia, tecnologia e privacidade, demonstrando a relevância da proteção de dados como princípio constitucional e de soberania nacional. O segundo capítulo aborda o poder da privacidade na era da informação e as implicações do colonialismo de dados sobre o Brasil, destacando as tensões entre o neoliberalismo global e a soberania digital. O terceiro capítulo foca no dever da ANPD em enfrentar o colonialismo de dados e garantir a adequação legislativa, enfatizando a necessidade de a ANPD emitir decisões de adequação para proteger os direitos e a soberania do Brasil no cenário global.

Palavras-chave: Proteção de dados; Transferência internacional de dados; ANPD; Soberania digital; Colonialismo de dados.

ABSTRACT

This work aims to deepen the study of the right to personal data protection in Brazil, focusing on international data transfers and the role of the National Data Protection Authority (ANPD) in issuing "adequacy decisions." The research proposes a critical analysis of the regulation of this matter, with particular attention to Resolution CD/ANPD nº 19/2024, which regulates the international transfer of personal data in Brazil, as provided for in the General Data Protection Law (LGPD). The thesis argues that the ANPD not only has the faculty but also the duty to issue such decisions to ensure that the personal data of Brazilians are adequately protected when transferred to countries with different legislation, avoiding that these data are processed in a manner incompatible with Brazilian standards. The research is structured into three chapters. The first explores the intersection between democracy, technology, and privacy, demonstrating the relevance of data protection as a constitutional and sovereignty principle. The second chapter addresses the power of privacy in the information age and the implications of data colonialism on Brazil, highlighting the tensions between global neoliberalism and digital sovereignty. The third chapter focuses on the ANPD's duty to confront data colonialism and ensure legislative adequacy, emphasizing the need for the ANPD to issue adequacy decisions to protect Brazil's rights and sovereignty in the global scenario.

Keywords: Data protection; International data transfer; ANPD; Digital sovereignty; Data colonialism.

RESUMEN

Este trabajo tiene como objetivo profundizar el estudio sobre el derecho a la protección de datos personales en Brasil, con énfasis en la transferencia internacional de datos y el papel de la Autoridad Nacional de Protección de Datos (ANPD) en la emisión de "decisiones de adecuación". La investigación propone un análisis crítico sobre la regulación de esta materia, con especial atención a la Resolución CD/ANPD nº 19/2024, que regula la transferencia internacional de datos personales en Brasil, conforme lo previsto en la Ley General de Protección de Datos (LGPD). La tesis defiende que la ANPD no solo tiene la facultad, sino también el deber de emitir tales decisiones para asegurar que los datos personales de los brasileños sean adecuadamente protegidos al ser transferidos a países con legislaciones diferentes, evitando que estos datos sean tratados de manera incompatible con los estándares brasileños. La investigación está estructurada en tres capítulos. El primero explora la intersección entre democracia, tecnología y privacidad, demostrando la relevancia de la protección de datos como principio constitucional y de soberanía nacional. El segundo capítulo aborda el poder de la privacidad en la era de la información y las implicaciones del colonialismo de datos en Brasil, destacando las tensiones entre el neoliberalismo global y la soberanía digital. El tercer capítulo se enfoca en el deber de la ANPD de enfrentar el colonialismo de datos y garantizar la adecuación legislativa, enfatizando la necesidad de que la ANPD emita decisiones de adecuación para proteger los derechos y la soberanía de Brasil en el escenario global.

Palabras clave: Protección de datos; Transferencia internacional de datos; ANPD; Soberanía digital; Colonialismo de datos.

LISTA DE ABREVIATURAS E SIGLAS

ABIN - Agência Brasileira de Inteligência

ANPD - Autoridade Nacional de Proteção de Dados

LGPD - Lei Geral de Proteção de Dados

RGPD - Regulamento Geral sobre a Proteção de Dados

IPED - Processador de Evidências Digitais

SUMÁRIO

1 INTRODUÇÃO	12
2 DEMOCRACIA E PROTEÇÃO DE DADOS PESSOAIS: UM PANORAMA CONTEMPORÂNEO	21
2.1 Importância da Democracia e sua relação com a proteção dos dados pessoais	21
2.2 O papel crucial da proteção de dados pessoais como princípio constitucional democrático	44
2.3 A tropicalização do pensamento sobre a proteção de dados pessoais	54
2.4 As tradições jurídicas, a “decisão de adequação” e o Brasil: entre traduções e “traições”	69
3 O PODER DA PRIVACIDADE, O NEOLIBERALISMO E O COLONIALISMO DE DADOS	76
3.1 O poder da privacidade e dos dados pessoais na era da informação.....	76
3.2 Colonialismo de dados	117
3.3 Neoliberalismo e imposições econômicas, políticas e culturais ao Sul Global	149
3.4 Brasil e os desafios frente ao poder, ao neoliberalismo e ao colonialismo de dados: a ANPD e a “decisão de adequação” nacional	172
4 O DEVER DA ANPD E A PROTEÇÃO DE DADOS PESSOAIS: A “DECISÃO DE ADEQUAÇÃO BRASILEIRA COMO RESPOSTA AO COLONIALISMO DE DADOS	176
4.1 O contexto da Lei Geral de Proteção de Dados.....	176
4.2 O processo legislativo da LGPD: inspirada ou submissa?	178
4.3 O texto da Lei Geral de Proteção de Dados	190
4.4 Uma comparação entre os textos normativos da LGPD e do RGPD: aspectos gerais.....	195
4.5 A “decisão de adequação” no direito brasileiro e europeu.....	203
4.6 Comparação LGPD vs RGPD: a “decisão de adequação”	222
4.7 O dever de uma “decisão de adequação” brasileira como resposta democrática ao poder da privacidade, ao neoliberalismo e ao colonialismo de dados.....	227
5 CONSIDERAÇÕES FINAIS: DESAFIOS E PERSPECTIVAS EMANCIPATÓRIAS – O NECESSÁRIO CONTROLE DE LEGALIDADE DO ART. 10 DA RESOLUÇÃO CD/ANPD Nº 19/2024	249
REFERÊNCIAS	264

1 INTRODUÇÃO

A produção bibliográfica, nacional e estrangeira, editada nos últimos anos sobre o direito à proteção de dados pessoais e os elementos a eles circundantes é prolífica, tributária da cada vez mais decisiva importância que a base econômica do mercado e da sociedade¹ tem atribuído à capacidade de captação, armazenamento e tratamento desses dados.

A busca por explicações do crescimento exponencial de uma tecnologia capaz de se ocupar, de maneira tão eficaz e agressiva, dos dados pessoais – explicada por um viés mais crítico e menos determinista, como a interação entre as dimensões da “razão” e da “experiência”, na forma pensada, v.g. por Andrew Feenberg², ou menos crítica e mais determinista, com a aceitação irrefletida de certos postulados técnicos, como a Lei de Moore dos Circuitos Integrados³ – ao tempo que de fundamental

¹ Como se tal cisão fosse possível se não por um elemento ideológico, imposto pelo totalitarismo neoliberal que coloniza todas as instituições sociais e políticas. Nesse sentido, Marilena Chauí: “De fato, o núcleo que define a forma totalitária é a homogeneização de todas as instituições sociais e políticas que, sendo idênticas, constituem um todo indivisível. No caso do totalitarismo neoliberal, todas as instituições sociais e políticas são consideradas organizações de um tipo determinado: a empresa. A escola, o hospital, a creche, as artes, o centro cultural, os cultos religiosos são empresas definidas pelas operações de mercado. Nessa perspectiva, Estado também é concebido como empresa e suas ações, definidas pelas regras do espaço privado, isto é, pelo mercado” (CHAUÍ, 2018, p. 420-421).

² Jan Hoogland *et al*, ao apresentarem o filósofo estadunidense, escrevem: “Andrew Feenberg é um dos filósofos mais conhecidos da tecnologia em nosso tempo. Ele estudou Filosofia na Universidade Johns Hopkins, na Universidade de Paris e da Califórnia. De 1969 a 2003, Feenberg foi professor de Filosofia da Tecnologia na Universidade Estadual de San Diego. Atualmente, ele ocupa a cadeira de chefe de pesquisa em Filosofia da Tecnologia na Universidade Simon Fraser no Canadá. Ele também foi convidado a palestrar em diversas universidades na Europa, no Japão e nos Estados Unidos. Com o passar do tempo, Feenberg mudou sua pesquisa da filosofia da tecnologia clássica para uma filosofia da tecnologia com orientações mais empíricas. No início de sua carreira, ele foi inspirado principalmente pelo filósofo Herbert Marcuse. Marcuse pertenceu à *Frankfurter Schule* (Escola de Frankfurt), um grupo bem conhecido de filósofos neomarxistas do século 20. Embora ele nunca tenha rejeitado essas influências, a maneira como foi articulada e fundada toda sua crítica da tecnologia foi progressivamente inspirada pelos estudos empíricos. (...) O que é significativo no pensamento de Feenberg a respeito da tecnologia é que o desenvolvimento de uma nova tecnologia não é determinado apenas pelas considerações técnicas-científicas. A tecnologia sempre tem algo indefinido: não se pode usar a dedução “lógica” no argumento técnico-científico na escolha do melhor projeto. Há outras considerações sociais que também entram em jogo. Desse modo, os desenvolvimentos técnicos são, em parte, determinados pelos agentes sociais, como as autoridades e os consumidores”. (HOOGLAND *et al*, 2018, p. 375-376)

³ Raymond Kurzweil, ex-engenheiro-chefe do Google, é um dos mais famosos entusiastas sobre o impacto da tecnologia na realidade humana. Em sua obra “A Era das Máquinas Espirituais”, escrita no ano de 1999, explicita sua visão determinista acerca do desenvolvimento da tecnologia, recorrendo, entre outros, à chamada Lei de Moore dos Circuitos Integrados: “Gordon Moore, inventor do circuito integrado e, posteriormente, presidente da Intel, observou, em 1965, que a área de superfície de um transistor (conforme embutida em um circuito integrado) estava sendo reduzida por, aproximadamente,

importância para uma escorreita compreensão da sociedade contemporânea e da normatividade atribuída a esses elementos pelo ordenamento jurídico, não tem recebido, por parte de importantes juristas brasileiros, mediante a competente redução sociológica⁴, a devida aclimação do pensamento.

Com efeito, ao se defrontar com a realidade decorrente da observância de um mundo muitas vezes hiperconectado⁵, cotejado à influência de escritos internacionais sobre o tema, parte dessa bibliografia nacional, a par de importantes contribuições para o pensamento jurídico pátrio, insiste em reproduzir, por vezes, a realidade alheia como a nossa. Há quem se utilize de exemplos talvez corriqueiros para os habitantes de países centrais⁶, mas impensáveis para a grande maioria do povo brasileiro⁷; há

30% a cada 12 meses. Em 1975, foi amplamente reportado que ele revisou essa observação para 18 meses. Moore afirma que sua atualização de 1975 foi para 24 meses, e isso parece ser mais adequado para os dados existentes. O resultado é que, a cada dois anos, você pode colocar duas vezes mais transistores num circuito integrado. Isso duplica tanto o número de componentes em um chip quanto sua velocidade. Já que o custo de um circuito integrado é razoavelmente constante, a implicação é que, a cada dois anos, você obtém duas vezes mais circuitos rodando ao dobro da velocidade pelo mesmo preço. Para muitas aplicações, esta é uma eficiente quadruplicação do valor. A observação se mantém verdadeira para todos os tipos de circuito, de chips de memória até processadores de computador. Essa inteligente observação se tornou conhecida como a Lei de Moore dos Circuitos Integrados, e o fenômeno notável da lei tem orientado a aceleração da informática nos últimos 40 anos". (KURZWEIL, 2007, p. 42-43). Nesse contexto, impende ressaltar que Kurzweil não reduz à Lei de Moore dos Circuitos Integrados; a identifica, em verdade, ao menos quatro outros paradigmas anteriores a esse. Nesse sentido: "o crescimento exponencial da computação não começou com a Lei de Moore dos Circuitos Integrados, mas remonta ao advento da computação elétrica, no início do século XX. (...) Então a Lei de Moore dos Circuitos Integrados não foi o primeiro, mas o quinto paradigma a continuar o crescimento exponencial da computação, hoje centenário. Cada novo paradigma chegou quando era necessário. Isto sugere que o crescimento exponencial não irá parar com o fim da Lei de Moore. Mas a resposta à nossa pergunta sobre a continuação do crescimento exponencial da computação é fundamental para nossa compreensão do século XXI". (*Ibidem*, p. 44-48).

⁴ O conceito foi criado por Guerreiro Ramos no séc. XX, em sua compreensão da sociologia enquanto atividade hermenêutica na qual as percepções sobre o mundo social influenciam a formulação de problemas e a abordagem de realidades sociais específicas. Essas perspectivas são moldadas pelas culturas nas quais estão inseridas; ocorre que toda cultura nacional é única, e essa singularidade cultural molda a forma como a sociologia aborda a realidade social. Nas palavras do autor: "A redução sociológica é um método destinado a habilitar o estudioso a praticar a transposição de conhecimentos e de experiências de uma perspectiva para outra. O que a inspira é a consciência sistemática de que existe uma perspectiva brasileira. Toda cultura nacional é uma perspectiva particular. Eis porque a redução sociológica é, apenas, modalidade restrita de atitude geral que deve ser assumida por qualquer cultura em processo de fundação (RAMOS, 1996, p. 42).

⁵ Termo criado pelos cientistas sociais canadenses Anabel Quan-Haase e Barry Wellman, por meio do qual conceituam uma sociedade em que as pessoas estão intimamente conectadas em razão do desenvolvimento da tecnologia da informação, responsável pelas importantes mudanças recentes nos meios de comunicação. (QUAN-HAASE; WELLMAN, 2003).

⁶ Na teoria dos sistemas mundiais, os países centrais (*core countries*) são os países capitalistas de que dependem os países periféricos (*peripheral countries*) e os países semi-periféricos (*semiperipheral countries*). Os países centrais controlam e se beneficiam do mercado global. Entre os que estudam o tema, destacam-se: Babones (2005); Wallerstein (2004); e Arrighi (2007).

⁷ Refere-se, nesse aspecto, à importante obra do jurista brasileiro Bruno Bioni, cuja introdução e visão geral se dá mediante a adaptação de um exemplo hipotético extraído do relatório do Conselho

quem ainda que se refira às assimetrias existentes entre os diferentes países no que toca ao nível de desenvolvimento tecnológico e de aproveitamento econômico dele decorrente, suscitando implicações no âmbito, v.g. dos conceitos de subdesenvolvimento e de soberania, o fazendo desacompanhada de uma crítica mais contundente e capaz de desvincular as noções de evolução e de progresso a de um posicionamento subserviente aos interesses estrangeiros, atribuindo alguma possibilidade de abrandamento da marginalização nacional não ao estímulo de sua autonomia e capacidade de resistência, mas ao fomento da inclusão digital dos cidadãos, a fim de que tenham aproveitadas sua mão de obra para os desígnios que lhe impõe os interesses alheios⁸; ou defenda que um futuro nacional benigno e proveitoso corresponda à eficaz reprodução do modelo praticado alhures⁹. E há quem simplesmente ignore, quase que por completo, a realidade nacional, sobre ela silenciando ao publicar seus escritos¹⁰.

A influência de teorias e estudos estrangeiros no pensamento nacional pode ser, de certo ângulo, compreendida. O fenômeno não é novo no Brasil. A história¹¹

Presidencial de Assessores de Ciência e Tecnologia dos Estados Unidos, em uma realidade distante da de milhões de brasileiros: “Taylor Rodriguez prepara-se para uma rápida viagem de negócios. Ela já arrumou a mala na noite anterior da sua partida e a deixou do lado de fora da casa, em frente à porta, para que alguém a apanhasse. Não há preocupação de que ela seja roubada, pois, além das câmeras das ruas estarem vigiando-a, cada item da sua mala possui etiquetas de radiofrequência. Eventual ladrão seria rastreado, juntamente com as roupas, e imediatamente detido. Quem vem apanhar a mala é a própria agência de viagens, mas que não necessitou das instruções com relação à data e hora, pois tais informações já haviam sido sincronizadas entre o calendário do smartphone de Taylor e o cadastro dela na agência. Na verdade, todo o itinerário da viagem está na nuvem – *cloud computing* –, de modo que a bagagem estará esperando por ela em seu hotel, no destino final da sua viagem”. (BIONI, 2018a, p. 29). De forma análoga, Sarmento e Castro, (2005, p. 19-21).

⁸ É o que deixa transparecer Patrícia Peck Pinheiro, ao defender que: “Outra consequência da sociedade convergente é o aumento da distância entre países desenvolvidos e em desenvolvimento, em razão do que se chama de analfabetismo digital — um problema político-social consistente em ter uma massa de trabalhadores não preparada para o uso das novas tecnologias. A preocupação não é apenas educacional: afeta a capacidade de aproveitamento de mão de obra, até mesmo de nível superior. O fenômeno de marginalização social se dá pela incapacidade dos indivíduos de conhecer e dominar as novas tecnologias — não basta saber escrever, é preciso saber enviar um e-mail. Ao mesmo tempo que a Era Digital abre maiores possibilidades de inclusão, a exclusão torna-se mais cruel. Aqueles que não tiverem existência virtual dificilmente sobreviverão também no mundo real, e esse talvez seja um dos aspectos mais aterradores dos novos tempos”. (PINHEIRO, 2021, p. 63-64).

⁹ Nesse sentido, a publicação de Bruno Bioni: “O Brasil não pode perder a chance de se tornar competitivo em uma economia de dados” (BIONI, 2018b).

¹⁰ Consoante se vê, v.g. na análise marcadamente expositiva e dogmática em Teixeira (2020).

¹¹ Sabe-se que, não raras vezes, a História do Direito coloca a si própria como questão teórica, uma vez que “da mesma maneira que não se pode falar levemente de “direito”, sem tornar preciso o que se quer dizer exatamente com isto, não se pode falar de “história” sem que um esclarecimento conceitual sobre esse termo seja requisitado” (FONSECA, 2010, p. 109). No entanto, além de unicamente se mencionar fatos do passado sobre os quais não há, entre os historiadores do direito,

recente da conformação do nosso ordenamento jurídico, com influências europeias no momento codificador¹² e no controle concentrado de constitucionalidade¹³, e estadunidense no controle difuso de constitucionalidade¹⁴, são exemplos importantes, ainda que não integrais, do que se afirma. E o próprio autor, em momento pretérito, ainda que tenha intuído a importância de se pensar o contexto brasileiro para se escrever (e, principalmente, se legislar) sobre o direito à proteção de dados pessoais¹⁵, não costurou inteiramente tais aspectos, já que não se dedicou, com a devida profundidade, a referido tema. Deve se considerar ainda que, em tempos anteriores, em que se desbravam os estudos sobre a privacidade, a influência estrangeira poderia ser a única fonte segura para se ancorarem estudos sobre um tema nascente, buscando-se em países com acesso mais amplo e facilitado às novidades tecnológicas – e, portanto, com o pensamento jurídico voltado a analisar

grandes controvérsias, o que se busca com esse recurso à história não é justificar o conteúdo da atual produção doutrinária; ao revés, o intuito é o de desnaturalizar qualquer compreensão que tome a história alheia como comutativa ou justificante da nossa. Acerca da utilização perniciosa da História do Direito em obras de dogmática jurídicas, novamente Fonseca: “A análise do passado do direito passa a servir para, ao afirmar a historicidade que é ínsita ao direito (que não é, portanto, algo que sobrepassa de modo isolado da realidade ou que é mero efeito da economia ou da política), demonstrar aos juristas das áreas da “dogmática jurídica” (civilistas, penalistas, processualistas etc.) que seus saberes, para serem bem manejados, dependem fundamentalmente de uma responsável análise diacrônica. Não mais uma mera e anacrônica “introdução histórica” – habitual nos manuais e mesmo nos trabalhos mais acadêmicos – que acentue principalmente as continuidades e permanências (frequentemente de modo artificial) ao longo do tempo, mas, ao contrário, a história do direito passa a demonstrar que uma análise teórica de qualquer dos “ramos do direito” deve ser atravessada pela história (visto que os conceitos e instituições jurídicas são, eles mesmos, embebidos de historicidade) e sua boa compreensão depende de sua inscrição temporal” (FONSECA, 2010, p. 36).

¹² Sobre a influência tardia do movimento codificador europeu sobre a ordem jurídica nacional – considerada, durante muito tempo, imune às transformações iniciadas com o Código Civil Napoleônico (1804), ver Andrade (1997).

¹³ Conforme lecionam Mendes e Branco: “Foi Rui Barbosa, talvez, quem primeiro percebeu, entre nós, que a sanção à violação do Texto Magno integra o próprio conceito de inconstitucionalidade” (2021, p. 2.316). Nesse sentido foi influenciado, no entanto, pelo filósofo austríaco do Direito, Hans Kelsen, idealizador da teoria do ordenamento jurídico disposto de forma hierárquica: “Daí afirmar-se que, para Kelsen, a jurisdição constitucional é uma decorrência lógica da Constituição em sentido estrito” (*Ibidem*, p. 2.318).

¹⁴ O controle de constitucionalidade estadunidense (judicial review), de caráter difuso, ganha sua conformação, a partir da qual influencia o ordenamento jurídico brasileiro, no célebre caso *Marbury vs. Madison* (1803), apesar de a gênese remota desse mecanismo jurídico ser anglo-saxônica. Sobre o tema: Matteucci (1998). Sobre a influência sobre a ordem jurídica nacional, ver Mendes e Branco (2021).

¹⁵ Assim se manifestou o autor em sua dissertação de Mestrado: “Se, por um lado, é certo que a realidade brasileira – visto que expoente de um país com proporções continentais, que abriga população culturalmente multifacetada e cuja desigualdade econômica e social atinge índices alarmantes – não pode ser completamente subsumida aos panoramas indicados pelos autores ao longo do trabalho, por outro se deve reconhecer sua imersão no contexto de uma “sociedade mundial em rede”, sofrendo, ainda, os importantes efeitos da “liquefação” social, sendo objeto de grande atenção no que toca à captação de dados pessoais” (FALK, 2017, p. 185).

as questões normativas delas decorrentes – orientações universitárias e bibliográficas para a realização de pesquisas acadêmicas¹⁶.

Na contemporaneidade, no entanto, não há espaço para omissão. A bibliografia crítica sobre a tecnologia é considerável, e há tempos já anunciava a carência de neutralidade no uso e conformação dos objetos técnicos. Da mesma forma, vai se tornando copiosa a doutrina nacional sobre o tema, em que se tornam possíveis vislumbrar seus diferentes erros e acertos. Deve-se ressaltar, ainda, a existência de algumas iniciativas voltadas a pensar, entre outros temas, a proteção de dados pessoais a partir de perspectivas pensadas pelo sul global¹⁷.

O propósito deste trabalho é aprofundar o entendimento dos estudos sobre o direito à proteção de dados pessoais no Brasil, no que toca à transferência internacional de dados pessoais. Para alcançar esse objetivo¹⁸, delineamos uma

¹⁶ Nesse contexto, figura de inestimável valor e inesquecível memória é a do Professor Dr. Danilo Doneda, reconhecido por suas significativas contribuições para o estudo da proteção de dados pessoais, e autor da clássica obra “Da privacidade à proteção de dados pessoais” (DONEDA, 2006), até hoje tida como um dos mais importantes referenciais de tantos trabalhos acadêmicos, e escrita enquanto fruto de seus estudos pioneiros realizados na Universidade de Camerino e na Autoridade Garante para a Proteção de Dados Pessoais, ambas na Itália.

¹⁷ Nesse sentido, a coletânea de artigos organizada por Eduardo Magrani (MAGRANI, 2017), coordenador da área de direito e tecnologia do ITS Rio, e que consiste em uma seleção abrangente de trabalhos que foram publicados no boletim “Digital Rights: América Latina e Caribe”, um projeto organizado no Brasil por Magrani e instituições da América Latina. Os artigos que compõem o livro destinado a pensar o “estado atual da sociedade latino-americana em relação à tecnologia e direitos digitais”, no entanto, por ironia do destino, estão todos em inglês. Nesse sentido: <https://itsrio.org/pt/publicacoes/direitos-digitais-latam/>. Acesso em: 02 ago. 2023.

¹⁸ Quanto à abordagem metodológica, é fundamental esclarecer nossa convicção. Em que pese nos alinhemos a uma concepção formal do fenômeno jurídico – reconhecendo, portanto, o aspecto normativo como condição *necessária* e *suficiente* para a formação de uma ordem jurídica (BOBBIO, 2010, p. 36) – o fazemos isentos de formalismos excessivos. Isso significa que, ao tempo em que admitimos a juridicidade dos textos normativos validamente incorporados ao ordenamento jurídico – caso, entre outras, da Lei nº 13.709/2018 e da Resolução CD/ANPD nº 19/2024 – nosso escopo nesse trabalho ultrapassa a dimensão da validade; aspiramos, portanto, contribuir para o debate jurídico e científico, enriquecendo-o com novas perspectivas que transitem pelos três elementos constitutivos da experiência jurídica, em uma visão não viciada pelo reducionismo. Nesse contexto, em sua obra “Teoria da Norma Jurídica”, Norberto Bobbio, ao lecionar sobre os três critérios de valoração das proposições normativas, assim se manifesta: “É claro que essa distinção de problemas não deve ser concebida como uma separação em compartimentos estanques. Quem quiser compreender a experiência jurídica nos seus vários aspectos deverá levar em conta que ela é aquela parte da experiência humana cujos elementos constitutivos são ideais de justiça a realizar, instituições normativas para realizá-los, ações e reações dos homens diante desses ideais e dessas instituições. Os três problemas são três diferentes aspectos de um único problema central, que é o problema da melhor organização da vida dos homens associados. Se insistimos na distinção e na independência das três valorações, é porque consideramos prejudicial a confusão entre elas, e sobretudo consideramos não ser possível aceitar outras teorias que não realizam essa distinção tão nitidamente, e tendem, ao contrário, a reduzir ora a um ora a outro dos três aspectos os outros dois, procedendo, como hoje se costuma dizer, com o reprovável neologismo da linguagem filosófica, com “reducionismo”. (BOBBIO, 2010, p. 45-46).

análise estruturada em três capítulos, que abordam aspectos cruciais acerca das questões jurídicas e políticas que permeiam a proteção de dados no contexto brasileiro, com um objetivo bem delineado: verificar em que medida a Autoridade Nacional de Proteção de Dados brasileira (ANPD) tem a faculdade, ou o dever, de emitir decisões de adequação.

A importância desse estudo se sobre-eleva em razão da recente aprovação, pelo Conselho Diretor da Autoridade Nacional de Proteção de Dados (ANPD), do Regulamento de Transferência Internacional de Dados. Referido regulamento, aprovado na forma de Resolução (Resolução CD/ANPD nº 19/2024), tem como objetivo disciplinar o contido no capítulo V da Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018), acerca da transferência internacional de dados pessoais, compreendendo, em referido capítulo, a redação do art. 33 ao art. 36 da LGPD.

Ocorre que, por mais que a LGPD seja explícita ao permitir a transferência internacional de dados pessoais somente para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao por ela previsto, e ao prescrever que o nível de proteção de dados do país estrangeiro ou do organismo internacional será avaliado pela autoridade nacional, referida Resolução, aprovada no mês de agosto de 2024, pelo Conselho Diretor da ANPD, expressamente define, em seu art. 10, a disponibilidade da ANPD sobre tal mister, ao prescrever que a ANPD *poderá* reconhecer, mediante decisão de adequação, a equivalência do nível de proteção de dados pessoais de país estrangeiro ou de organismo internacional com a legislação nacional de proteção de dados pessoais – sem, no entanto, obrigá-la a fazê-lo.

Não se trata, apenas, de um alerta acerca de eventual incompatibilidade semântica entre os vocábulos *somente*, *será* e *poderá* – ainda que também dotado de devida importância na análise da incompatibilidade do contido na Resolução com o prescrito da LGPD, levando em conta sua função de regulamentação e orientação infralegal – mas de responsabilidade maior: a consciência de que, sobre tal véu gramatical, se esconde uma pujante tomada de posição capaz de impactar a própria vivência democrática e a soberania nacional.

Com essa finalidade, o primeiro capítulo tem como objetivo situar a discussão no contexto da interseção entre a democracia e a proteção de dados pessoais. A partir

da análise de teorias contemporâneas sobre o impacto das tecnologias digitais na vida política e social, o capítulo busca destacar a importância da proteção de dados como um princípio constitucional democrático. Será explorado como a privacidade e o controle sobre dados pessoais se tornaram essenciais para a autonomia individual e para a manutenção da soberania popular, fundamentos da democracia moderna.

A subseção 2.1 discutirá a importância da democracia na contemporaneidade, bem como a relação entre democracia e os dados pessoais, destacando como a transformação digital afeta os princípios democráticos, em especial no tocante à proteção de dados. Em 2.2, será abordado o papel da proteção de dados como princípio constitucional, evidenciando sua relevância para garantir que o cidadão possa exercer seus direitos com segurança no ambiente digital. A subseção 2.3 introduzirá o conceito de “tropicalização” da proteção de dados, abordando como o Brasil é afetado pela conjuntura internacional de transferência e exploração econômica e política de dados pessoais, com a necessidade de o pensamento estrangeiro ser adaptado às realidades e especificidades brasileiras. Em 2.4, será analisada a interrelação entre a legislação alienígena e a nacional, a fim de perceber de que maneira as exigências da legislação europeia e a necessidade de harmonização com padrões internacionais de proteção de dados influenciam a “tradução” da legislação estrangeira para a brasileira, no que diz respeito à “decisão de adequação” doméstica acerca da equivalência do nível de proteção de dados pessoais de país estrangeiro ou de organismo internacional com a legislação nacional de proteção de dados pessoais.

No segundo capítulo, o foco se voltará ao poder da privacidade e às dinâmicas globais de controle de dados. A subseção 3.1 discutirá o papel da privacidade na era da informação, analisando como a capacidade de proteger dados pessoais se tornou uma questão central no enfrentamento do poder exercido pelos entes estatais e pelas grandes corporações tecnológicas. Em seguida, a subseção 3.2 introduzirá o conceito de colonialismo de dados, examinando como o Brasil tem enfrentado a exploração de seus dados no cenário global. Em 3.3, será abordado o impacto do neoliberalismo sobre as políticas de proteção de dados, particularmente as imposições econômicas, políticas e culturais que afetam o Sul Global. Por fim, em 3.4, serão discutidos os desafios que o Brasil enfrenta no combate aos elementos supramencionados e como

a Autoridade Nacional de Proteção de Dados – ANPD, por meio da emissão de "decisões de adequação", pode proteger os interesses nacionais e garantir a soberania digital.

O terceiro capítulo focará no dever da ANPD em relação à proteção de dados pessoais no Brasil, abordando a "decisão de adequação" como resposta ao poder da privacidade, ao neoliberalismo e ao colonialismo de dados. A subseção 4.1 apresentará o contexto da criação da Lei Geral de Proteção de Dados (LGPD), destacando seu papel na regulação da privacidade e da proteção de dados no Brasil. Em 4.2, será analisado o processo legislativo que resultou na LGPD, discutindo se a lei foi inspirada em modelos estrangeiros – mormente o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia – ou se houve submissão às suas exigências. A subseção 4.3 explorará o texto da LGPD em detalhes, comparando-o com o RGPD, e destacando as principais semelhanças e diferenças entre os dois. Em 4.4 e 4.5, a discussão sobre a “decisão de adequação” será aprofundada, com ênfase no papel dessa decisão para garantir que o Brasil possa transferir dados pessoais internacionalmente sem prejudicar sua soberania. Em 4.6, será discutido o dever da ANPD de emitir "decisões de adequação", apresentando-as como um imperativo necessário para enfrentar o colonialismo de dados – e, portanto, a consequente imprestabilidade da redação hoje atribuída ao art. 10 da Resolução CD/ANPD nº 19/2024. Por fim, nas considerações finais, se analisará os desafios e as perspectivas emancipatórias no contexto da proteção de dados no Brasil, sugerindo que a atuação assertiva da ANPD pode transformar o país em um protagonista autônomo na regulação global de dados, desde que estabeleça um marco regulatório que proteja o Brasil da exploração de dados por potências estrangeiras, enfatizando a necessidade de uma ação assertiva e estratégica para garantir a soberania digital brasileira.

A conclusão reiterará a importância da proteção de dados como um direito fundamental no Brasil, reconhecido pela Emenda Constitucional 115/2022, e o papel central da ANPD na emissão de "decisões de adequação" como instrumento de proteção da soberania nacional e dos direitos individuais dos cidadãos brasileiros. A tese defenderá que a proteção de dados pessoais deve ser vista como uma extensão dos direitos fundamentais em um Estado Democrático de Direito e como uma ferramenta essencial para a proteção da soberania nacional em um mundo digital

globalizado. A ANPD, como responsável pela aplicação e regulamentação da LGPD, deve não apenas reconhecer, mas também cumprir com seu dever de proteger os dados pessoais dos brasileiros, assegurando que o país se posicione de maneira soberana e equitativa no cenário internacional de proteção de dados – o que significa o compromisso com um dever de emissão de “decisões de adequação” com vistas aos impactos na proteção das individualidades e coletividades brasileiras, em fortalecimento da democracia nacional.

Com efeito, a Autoridade Nacional de Proteção de Dados (ANPD) ocupa um papel central nesse processo de defesa da soberania e proteção da privacidade no Brasil. A ANPD não apenas tem a faculdade, portanto, mas, conforme se argumenta, o dever de emitir decisões de adequação que garantam que legislações estrangeiras sejam compatíveis com os marcos de proteção de dados brasileiros. Isso não pode ser visto como uma prerrogativa facultativa; trata-se de um imperativo para assegurar que a transferência internacional de dados pessoais ocorra de forma justa, protegendo tanto os direitos individuais dos cidadãos brasileiros quanto os interesses nacionais. Tal medida é essencial para evitar que dados sensíveis de brasileiros sejam tratados sob legislações mais flexíveis, potencialmente abusivas ou inadequadas, com graves consequências para a democracia e a autonomia nacional.

2 DEMOCRACIA E PROTEÇÃO DE DADOS PESSOAIS: UM PANORAMA CONTEMPORÂNEO

2.1 Importância da Democracia e sua relação com a proteção dos dados pessoais

No dia 05 de outubro de 2023, a Constituição da República Federativa do Brasil completou 35 anos de vigência ininterrupta. O Supremo Tribunal Federal – a quem compete, constitucional e precipuamente, a guarda da Constituição (CF, art. 102, *caput*) – inaugurou, a fim de celebrar a data, no dia 20 de setembro de 2023, a exposição “35 anos da Constituição Federal de 1988”. Durante o evento, foi lançado o livro “O Olhar dos Ministros do Supremo Tribunal Federal sobre a Constituição Cidadã”, obra coletiva, composta por dezoito artigos, escritos por Ministras e Ministros aposentados e da atual composição do STF.

A então presidente do Supremo Tribunal Federal, Ministra Rosa Weber, ao discursar durante a abertura da exposição¹⁹, afirmou que: “A Constituição de 1988 é fruto da redemocratização e da instituição da ordem democrática do país”²⁰. Ao encerrar a cerimônia, citou o discurso do Presidente da Assembleia Nacional Constituinte, Ulysses Guimarães: “a persistência da constituição é a sobrevivência da democracia”²¹.

¹⁹SUPREMO TRIBUNAL FEDERAL. **Exposição no STF comemora 35 anos da Constituição Federal**. Disponível em: <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=514477&ori=1#:~:text=Exposi%C3%A7%C3%A3o%20no%20STF%20comemora%2035%20anos%20da%20Constitui%C3%A7%C3%A3o%20Federal&text=A%20presidente%20do%20Supremo%20Tribunal,da%20Constitui%C3%A7%C3%A3o%20Federal%20de%201988%E2%80%9D>. Acesso em: 23 dez. 2023.

²⁰ Este ano de 2023 marca os 35 anos da Constituição Federal, a nossa Constituição Cidadã, promulgada em 05 de outubro de 1988, fruto da redemocratização do Brasil e instituidora da ordem democrática em que vivemos desde então”. E encerra com: “O livro visa a propiciar ainda conhecimento e informação sobre o mais elevado documento da história brasileira, que, em três décadas e meia de vigência, permite desfrutarmos o Estado democrático de direito em sua plenitude.” SUPREMO TRIBUNAL FEDERAL. **O olhar dos Ministros do Supremo Tribunal Federal sobre a Constituição Cidadã**. Brasília: STF, Secretaria de Altos Estudos, Pesquisas e Gestão da Informação, 2023. 250 p. Disponível em: https://www.stf.jus.br/arquivo/cms/publicacaoPublicacaoInstitucionalComemoracoes/anexo/CF35anos_artigos.pdf. Acesso em: 23 dez. 2023

²¹ Discurso proferido na sessão de 5 de outubro de 1988, publicado no DANC de 5 de outubro de 1988, p. 14380-14382. Reproduz-se, ante a absoluta pertinência da fala do Presidente da Assembleia Nacional Constituinte de 1987–1988, um trecho maior de seu discurso, excluídas as notas taquigráficas

As repetidas menções à democracia não são acidentais. A partir das 15h50min do dia 5 de outubro de 1988, a democracia voltou a vigorar no Brasil, após 21 anos do golpe de estado que aqui instaurou um ilegítimo e detestável regime militar. Some-se a isso o fato de esse período representar, em 524 anos de cronologia pós-invasão²², o maior período democrático contínuo de nossa história²³.

O anúncio do retorno da democracia não se mostra suficiente, *per sí*, para que se atribua a ele um valor epistêmico benfazejo. Seria mesmo possível imaginar a

referentes às reações dos demais constituintes: “A Constituição certamente não é perfeita. Ela própria o confessa, ao admitir a reforma. Quanto a ela, discordar, sim. Divergir, sim. Descumprir, jamais. Afrontá-la, nunca. Traidor da Constituição é traidor da Pátria. Conhecemos o caminho maldito: rasgar a Constituição, trancar as portas do Parlamento, garrotear a liberdade, mandar os patriotas para a cadeia, o exílio, o cemitério. A persistência da Constituição é a sobrevivência da democracia. Quando, após tantos anos de lutas e sacrifícios, promulgamos o estatuto do homem, da liberdade e da democracia, bradamos por imposição de sua honra: temos ódio à ditadura. Ódio e nojo. Amaldiçoamos a tirania onde quer que ela desgrace homens e nações, principalmente na América Latina”. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/plenario/discursos/escrevendohistoria/25-anos-da-constituicao-de-1988/constituente-1987-1988/pdf/Ulysses%20Guimaraes%20-%20DISCURSO%20%20REVISADO.pdf>. Acesso em: 23 dez. 2023.

²² Os termos comumente empregados para designar o ano em que aqui aportaram os tripulantes das nove naus, três caravelas e uma naveta de mantimentos capitaneadas pelo português Pedro Álvares Cabral são, entre outros, “descobrimento”, “achamento” e “invasão”. Darcy Ribeiro (1995) é um exemplo de autor que se utiliza de ambos os termos para se referir a esse evento – optando, no entanto, por uma questão de sinceridade epistêmica, pelo último, ante a utilização reiterada dos termos “invasão” e “invasor”, e não “descobrimento” ou “achamento”, e mesmo “descobridor” ou “achador”, para se referir à data de chegada da armada, e aos próprios lusitanos, no Brasil. Nesse sentido, Ribeiro: “Nas décadas do achamento, descoberta ou invasão do Brasil, surgiram descrições cada vez mais minuciosas das novas terras. Assim, elas iam sendo apropriadas pelo invasor também pelo conhecimento de seus rios e matas, povos, bichos e duendes” (1995, p. 56). Também: “É de todo provável que alcançasse, ou pouco excedesse, a cinco milhões o total da população indígena brasileira quando da invasão” (RIBEIRO, 1995, p. 141). E, por fim: “O Brasil e os brasileiros, sua gestação como povo, é o que trataremos de reconstituir e compreender nos capítulos seguintes. Surgimos da confluência, do entrelaçamento e do caldeamento do invasor português com índios silvícolas e campineiros e com negros africanos, uns e outros aliados como escravos”. (RIBEIRO, 1995, p. 19).

²³ Nesse sentido, há uma valoração como “insuficiente” da democracia experimentada no período conhecido como República Velha ou Primeira República, compreendido entre 1889, data da Proclamação da República, e 1930, início da “Era Vargas”. Nesse ínterim, o Brasil esteve sob um regime de democracia restrita, caracterizado pelo sufrágio censitário, pela persistência de práticas autoritárias no Executivo e pela presença de fraudes e intimidações eleitorais. A contestação política nacional era praticamente ausente, uma vez que o poder estava concentrado em acordos internos entre as elites, um cenário comumente descrito como “política dos governadores”, enquanto as eleições estavam distantes dos critérios de integridade e competitividade que definem um regime plenamente democrático (BIZZARRO, FERNANDO; COPPEDGE, MICHAEL, 2017, p. 9). O outro período foi o de 1946 a 1964, inaugurado pela Constituição de 1946 e encerrado com o golpe militar que dá início à Ditadura Militar. Sobre a atualidade, correspondente ao intervalo de 1985 até o presente, em que a redemocratização ocorre gradualmente após o regime militar, culminando com a eleição indireta de Tancredo Neves em 1985 e a promulgação da Constituição de 1988, que estabelece a atual ordem democrática, leciona Luís Roberto Barroso: “Desde o fim do regime militar e, sobretudo, tendo como marco histórico a Constituição de 1988, o Brasil vive o mais longo período de estabilidade institucional de sua história”. BARROSO, O Constitucionalismo democrático como ideologia vitoriosa no séc. XX, *in* Revolução tecnológica, crise da democracia e Constituição: direito e políticas públicas num mundo em transformação, p. 73. Sobre o assunto, ver também: VILLA, 2011, p. 82-113.

comemoração de um retorno, ou implantação, de outros regimes políticos, como autocráticos ou ditatoriais²⁴? A resposta óbvia é que a democracia requer uma fundamentação mais robusta que justifique sua importância. A pergunta “por que a democracia importa?”, ao se colocar como relevante, exige que lhe forneçamos uma resposta, ainda que de conteúdo mínimo, clara e bem sustentada²⁵. Essa resposta, por mais que sem pretensão exaustiva, deve contemplar os valores e princípios que a democracia representa, como a garantia dos direitos fundamentais e a participação ativa dos cidadãos na formação do poder político²⁶. E, mais especificamente, no âmbito da proteção dos dados pessoais, considerar como os princípios democráticos, como a transparência, a responsabilização e a participação cidadã, contribuem para a criação de marcos regulatórios condizentes e eficazes, entre outros, na transferência internacional de dados, garantindo a proteção dos direitos individuais e coletivos.

Esse aspecto é, inclusive, crucial para a compreensão, o estabelecimento e a defesa da democracia na contemporaneidade: a relação entre a proteção dos dados pessoais e a Democracia. Consoante se verificará, a captura e o tratamento de dados pessoais por organismos estrangeiros, mormente no âmbito do que se tem convencionalmente chamado de "colonialismo de dados", representa uma séria ameaça à

²⁴ Como de quando em quando fazem, ao arpejo da Constituição Cidadã, as forças armadas brasileiras, ao publicarem mensagens comemorativas do golpe militar de 31 de março de 1964 — como fez o Ministério da Defesa no ano de 2020, ao editar uma “Ordem do Dia Alusiva ao 31 de março de 1964”. A ordem do dia é um documento em que a autoridade militar divulga orientações, homenagens, instruções, reflexões e posicionamentos sobre eventos importantes. O ato veiculava mensagem comemorativa dos 56 anos do último golpe militar, e foi objeto de uma ação popular, a partir da qual o Plenário do Supremo Tribunal Federal firmou entendimento, julgado sob o rito da repercussão geral (Tema 1322), de que é inconstitucional o uso de recursos públicos para promover comemorações ao golpe militar de 1964, pois se trata de ato lesivo ao patrimônio imaterial da União. A tese de repercussão geral firmada foi a seguinte: “A utilização, por qualquer ente estatal, de recursos públicos para promover comemorações alusivas ao Golpe de 1964 atenta contra a Constituição e consiste em ato lesivo ao patrimônio imaterial da União”. Nesse sentido: <https://noticias.stf.jus.br/postsnoticias/recursos-publicos-nao-podem-ser-utilizados-para-promover-comemoracoes-do-golpe-de-1964-decide-stf/>.

Acesso em: 29 set. 2024.

²⁵ Semelhante compreensão foi destacada por Gabriel Avila Casalecchi, em sua obra de ciência política “Legado Democrático e apoio à democracia na América Latina: evidências e mecanismos explicativos” (CASALECCHI, 2018). Referida obra recebeu o prêmio “melhor tese ABCP 2018”. “Não é nosso propósito verticalizar um tema já tão discutido na literatura, com diferentes vertentes e posições (COLLIER; LEVITSKY, 1997). Por outro lado, não podemos nos eximir de assumir uma posição dentro desse debate, sob o risco de permanecer na esterilidade conceitual que hoje ronda a ideia de democracia. Nesse sentido, endossamos aqui posição semelhante à de Bobbio (1994), Dahl (1997) e Mainwaring, Brinks e Pérez-Liñán (2001), que reivindicam uma definição ‘mínima’ de democracia. Uma definição é mínima na medida em que é suficiente — ainda que não exaustiva — para determinar as propriedades ou características essenciais de uma coisa ou ser, sem as quais este não existiria ou se confundiria com outro” (p. 20).

²⁶ A fim de evitar uma sub-representação. Nesse sentido, Casalecchi, p. 21.

soberania dos Estados e à autonomia dos cidadãos. O colonialismo de dados ocorre quando grandes corporações ou Estados estrangeiros obtêm e exploram dados pessoais de cidadãos de outros países sem a devida regulamentação ou consentimento, comprometendo a privacidade, a autodeterminação informacional e os direitos fundamentais dessas populações. Esse fenômeno fere diretamente os princípios democráticos, como a transparência, a responsabilização e a participação cidadã, na medida em que transfere o controle dos dados para entidades que não respondem democraticamente aos cidadãos afetados, minando o papel do Estado como garantidor dos direitos e diluindo o poder do povo na tomada de decisões que afetam suas vidas. Assim, a proteção e regulamentação da transferência internacional de dados pessoais emergem como questões centrais para a preservação da democracia, pois garantem que os direitos dos cidadãos sejam respeitados em um cenário globalizado, onde a informação se tornou um dos principais ativos de poder.

Em verdade, uma primeira resposta supostamente suficiente para uma análise estritamente normativa do ordenamento jurídico brasileiro residiria em um estudo de natureza rigorosamente formal: o artigo 1º da Constituição da República Federativa do Brasil estabelece que a organização do Estado se dá sob a forma de um Estado Democrático de Direito²⁷. A importância do instituto e sua consequente proteção, portanto, se revelaria, tão somente, pela opção feita pelo legislador, cognoscível mediante a interpretação do que apregoa o texto normativo; no entanto, assim como

²⁷ Nesse sentido, Luís Roberto Barroso: “O Estado moderno se consolida, ao longo do século XIX, sob a forma de Estado de direito. Na maior parte dos países europeus, a fórmula adotada foi a monarquia constitucional. O núcleo essencial das primeiras constituições escritas é composto por normas de repartição e limitação do poder, aí abrangida a proteção dos direitos individuais em face do Estado. A noção de democracia somente viria a desenvolver-se e aprofundar mais adiante, quando se incorporam à discussão ideias como fonte legítima do poder e representação política. Apenas quando já se avançava no século XX é que seriam completados os termos da complexa equação que traz como resultado o Estado democrático de direito: quem decide (fonte do poder), como decide (procedimento adequado) e o que pode e não pode ser decidido (conteúdo das obrigações negativas e positivas dos órgãos de poder). A construção do Estado constitucional de direito ou Estado constitucional democrático, no curso do século XX, envolveu debates teóricos e filosóficos intensos acerca da dimensão formal e substantiva dos dois conceitos centrais envolvidos: Estado de direito e democracia. Quanto ao Estado de direito, é certo que, em sentido formal, é possível afirmar sua vigência pela simples existência de algum tipo de ordem legal cujos preceitos materiais e procedimentais sejam observados tanto pelos órgãos de poder quanto pelos particulares. Este sentido mais fraco do conceito corresponde, segundo a doutrina, à noção alemã de *Rechtsstaat*, flexível o suficiente para abrigar Estados autoritários e mesmo totalitários que estabeleçam e sigam algum tipo de legalidade. Todavia, em uma visão substantiva do fenômeno, não é possível ignorar a origem e o conteúdo da legalidade em questão, isto é, sua legitimidade e sua justiça. Esta perspectiva é a que se encontra subjacente ao conceito anglo-saxão de *rule of law* e que se procurou incorporar à ideia latina contemporânea de Estado de direito, *État de droit*, *Stato di diritto*, *Estado de derecho*”. BARROSO, 2013, p. 62-63.

optara pela qualidade de “democrático”, poderia ter agido de forma diversa, alcunhando ao Estado de Direito outra característica²⁸.

Essa opção formal reflete, no entanto, também uma escolha política que traz importantes consequências às ações tomadas pelos poderes do Estado, seja em suas funções típicas ou atípicas. Essa opção implica que o Brasil adote um modelo jurídico que garanta a supremacia da Constituição e a observância de seus princípios fundamentais, assegurando que o funcionamento das instituições e a proteção dos direitos individuais e coletivos se realizem dentro dos limites constitucionais. Mas não só: indica, outrossim, que a própria legitimidade do poder estatal emana do povo, conforme estabelecido no artigo 1º da Constituição da República Federativa do Brasil, que afirma que "todo o poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente, nos termos desta Constituição." Assim, ao adotar o modelo de Estado Democrático de Direito, o Brasil não apenas assegura a supremacia da Constituição, mas reafirma que o povo é a fonte primária do poder político²⁹, seja por meio de seus representantes ou por mecanismos de participação direta, como plebiscitos e referendos.

Esquadrinhar profundamente os aspectos constitucionais que envolvem o conceito demandaria uma incursão na própria história do Constitucionalismo – ou Constitucionalismos, nos ditames de Canotilho³⁰. Não há dúvida que a totalidade das

²⁸ Nesse sentido, Dimitri Dimoulis (2020) leciona que: “O constituinte brasileiro compreende o conceito de Estado de direito no sentido formal. A Constituição Federal qualifica a República como um ‘Estado democrático de direito’ (art. 1º, *caput*). O adjetivo ‘democrático’ foi colocado justamente porque o constituinte entendia que a simples referência ao ‘Estado de direito’ não garante a natureza democrática do regime” (p. 93).

²⁹ Esse fundamento político, ao vincular diretamente a democracia à vontade popular, reforça a importância de assegurar que o Estado atue em nome e para o benefício do povo, respeitando e promovendo os direitos fundamentais, a justiça social e a igualdade de condições para todos os cidadãos. A democracia, portanto, não se restringe a um conjunto de normas formais, mas a um compromisso contínuo com a participação cidadã e a proteção dos direitos, elementos cruciais para o fortalecimento das instituições e a preservação da legitimidade do poder.

³⁰ O jurista português promove uma importante distinção entre o *constitucionalismo* (moderno) enquanto conceito abstrato e nunca verificado empiricamente, com simples função operacional no estudo do Direito Constitucional, e os distintos *constitucionalismos*, dispostos a apreender as nuances dos distintos movimentos constitucionais compreensíveis tão apenas ao se compulsar a história constitucional de distintos entes políticos. Nesse sentido, Canotilho: “O movimento constitucional gerador da constituição em sentido moderno tem várias raízes localizadas em horizontes temporais diacrônicos e em espaços históricos geográficos e culturais diferenciados. Em termos rigorosos, não há um constitucionalismo, mas vários constitucionalismos (o constitucionalismo inglês, o constitucionalismo americano, o constitucionalismo francês). Será preferível dizer que existem diversos movimentos constitucionais com corações nacionais, mas também com alguns momentos de

conquistas civilizatórias advindas da limitação do poder do Estado mediante a consolidação do Estado moderno, no século XIX, como Estado de Direito, desempenham um importante papel na conformação da contemporaneidade³¹.

As primeiras constituições, em verdade, se concentravam na limitação do poder e na proteção dos direitos individuais. A noção de democracia, envolvendo a fonte legítima do poder e a representação política, só foi plenamente desenvolvida no século XX, quando se estabeleceu o conceito de Estado Democrático de Direito, que define quem detém o poder, como ele é exercido e quais os seus limites. Esse processo gerou intensos debates sobre as dimensões formal e substantiva do Estado de Direito. A visão formal, exemplificada pela noção de *Rechtsstaat*, permite a vigência de uma legalidade mesmo em Estados autoritários, enquanto a visão substantiva, como no conceito de *rule of law*, enfatiza a legitimidade e a justiça da ordem legal (BARROSO, 2018, p. 42).

Uma análise profunda em cada percurso constitucional moderno desbordaria dos objetivos do presente escrito. Apostar em uma definição que ultrapasse a mera constatação da exigência formal do caráter democrático, no entanto, se mostra desejável, e significa, inicialmente, ciente dos debates ínsitos à densificação do próprio instituto, uma postura de humildade perante um conceito que, ao longo dos

aproximação entre si, fornecendo uma complexa tessitura histórico-cultural. E dizemos ser mais rigoroso falar de vários movimentos constitucionais do que de vários constitucionalismos porque isso permite recortar desde já uma noção básica de constitucionalismo. Constitucionalismo é a teoria (ou ideologia) que ergue o princípio do governo limitado indispensável à garantia dos direitos em dimensão estruturante da organização político-social de uma comunidade. Neste sentido, o constitucionalismo moderno representará uma técnica específica de limitação do poder com fins garantísticos. O conceito de constitucionalismo transporta, assim, um claro juízo de valor” (2007, p. 51).

³¹ As considerações anteriores justificarão, ainda hoje, a indispensabilidade de um conceito histórico de Constituição. Nesse sentido, ganha crédito a abordagem de Luís Roberto Barroso, ao discorrer sobre o constitucionalismo no início do séc. XXI. Com efeito, o Ministro do Supremo Tribunal Federal evidencia a consolidação do Estado moderno como Estado de direito ao longo do século XIX. As primeiras constituições escritas destacaram normas de repartição e limitação do poder, abrangendo a proteção dos direitos individuais frente ao Estado. A evolução para o Estado democrático de direito, ao longo do século XX, envolveu debates intensos sobre a dimensão formal e substantiva dos conceitos centrais de Estado de direito e democracia. Barroso destaca a complexidade da equação que resulta no Estado democrático de direito, incorporando a compreensão dos termos: quem decide, como decide e o que pode ou não ser decidido. No contexto do Estado de direito, a perspectiva substantiva, ligada à origem, legitimidade e justiça da legalidade, torna-se crucial. Quanto à democracia, a visão material, além do governo da maioria, implica o governo para todos, incluindo minorias e grupos politicamente menos expressivos. O constitucionalismo democrático, na primeira década do século XXI, continua a enfrentar desafios na conciliação entre soberania popular e direitos fundamentais, buscando o equilíbrio entre governo da maioria e garantia de uma vida digna e livre para todos, dentro de um contexto de justiça, pluralismo e diversidade. Este projeto permanece relevante para o milênio, representando uma aspiração significativa na busca por uma ordem democrática justa e inclusiva. (2018, p. 41-42).

tempos e lugares, adquiriu distintas conotações e nuances. De fato, segundo Jean-Paul Gagnon (2018), da Universidade de Camberra, existem mais de 2.000 tipos de democracia (2.234, para ser exato), o que revela a complexidade de se enquadrar esse regime em uma única definição universal. Além disso, há de se reconhecer que, no séc XXI, a par de Estados que não fazem qualquer questão de sustentar seus regimes políticos em bases democráticas, há vários que se anunciam democráticos, com concepções distintas do que significa esse termo. A depender da definição e da métrica empregada, inclusive, há como se fazer uma gradação da qualidade da democracia vivida em cada país – à exemplo da ferramenta *Democracy Matrix*, mantida pelo Instituto de Ciência Política e Sociologia da *Julius-Maximilians-Universität Würzburg*, Alemanha³². Com efeito, de acordo com a classificação apresentada pela Universidade, apenas 35 (trinta e cinco) países possuem uma "working democracy", enquanto outros são classificados como "deficient democracies" – inclusive o Brasil, que ocupa o 75º lugar do ranking – "hybrid regimes", ou até mesmo "moderate autocracies" e "hard autocracies". (<https://www.democracymatrix.com/ranking>).

Ademais, conforme ainda Barroso, "o constitucionalismo democrático foi a ideologia vitoriosa do século XX"³³ (BARROSO, 2018, p. 288). Nesse arranjo

³² A *Democracy Matrix* é uma ferramenta desenvolvida para medir a qualidade da democracia em diferentes países ao redor do mundo, cobrindo um período que vai de 1900 até 2019. Essa ferramenta se destaca por oferecer uma análise detalhada e fundamentada na teoria democrática, dividida em três dimensões principais: liberdade política, igualdade política e controle político e jurídico. Essas dimensões são analisadas em conjunto com cinco instituições-chave que estruturam o funcionamento da democracia, resultando em 15 campos de análise. A combinação desses elementos permite uma avaliação profunda da democracia, levando em conta diferentes aspectos que afetam seu funcionamento. A medição da democracia passa por três fases principais: a conceitualização, a operacionalização e a agregação. Na fase de conceitualização, define-se uma democracia de acordo com uma árvore conceitual que oferece clareza e discriminação entre os diferentes componentes da democracia. Já na fase de operacionalização, indicadores empíricos são atribuídos a cada componente, utilizando-se, para isso, a base de dados *Varieties of Democracy (V-Dem)*, que oferece uma vasta gama de variáveis. A fase de agregação, por sua vez, reúne os valores medidos, permitindo a determinação da qualidade democrática não apenas de um país como um todo, mas também de suas instituições específicas e dimensões. Um dos grandes diferenciais da *Democracy Matrix* é que, além de fornecer um valor global da qualidade democrática, ela permite a criação de perfis de democracia, distinguindo entre democracias libertárias, igualitárias ou focadas no controle. A ferramenta também classifica os regimes em um contínuo que vai de democracias plenas a autocracias extremas, passando por regimes híbridos e democracias deficientes. Assim, a *Democracy Matrix* oferece uma visão altamente detalhada e diferenciada da qualidade democrática, com implicações tanto para a ciência política quanto para a política internacional e as políticas de desenvolvimento. Disponível em: <https://www.democracymatrix.com/>. Acesso em: 24 dez. 2023.

³³ Barroso, ainda sobre o constitucionalismo democrático, indica que a vitória de referido projeto representa, em verdade, uma visão material de mundo, já que: "nele se condensam as promessas da

institucional, há a fusão de duas tradições que percorreram caminhos distintos: o constitucionalismo e a democracia, que coexistem em uma tensão criativa. O constitucionalismo, originado da tradição liberal do final do século XVII, sustenta a ideia de limitação do poder pelo Direito e de respeito aos direitos fundamentais. Ele propõe que nenhum governo, mesmo que eleito, pode atuar fora dos limites impostos pela Constituição. Já a democracia expressa a soberania popular e o governo da maioria, consolidando-se ao longo do século XX com a universalização do sufrágio e a eliminação das restrições à participação política baseadas em critérios de riqueza, gênero ou raça. A tensão entre essas duas ideias é inerente ao fato de que, enquanto o constitucionalismo visa frear o poder, a democracia busca amplificar a voz popular. O desafio é equilibrar o governo da maioria com a proteção dos direitos fundamentais e das minorias, garantindo que a soberania popular não se traduza em tirania da maioria, e que o respeito ao Direito não engesse a vontade democrática (*Idem*).

A raiz do termo "democracia" remonta ao grego antigo, no qual "*demos*" significa povo, e "*kratos*" significa poder ou governo. Etimologicamente, portanto, democracia pode ser traduzida como "governo do povo" ou "poder do povo" (AIETA, 2014; CHAÚÍ, 2018). Contudo, essa definição literal, embora clara, não abrange a complexidade do conceito ao longo da história e nas diferentes tradições políticas. Segundo Aieta, a palavra "*demos*", no contexto grego clássico, apresentava diferentes significados, incluindo "muitas pessoas" ou até "as classes mais pobres" da sociedade, o que demonstra desde cedo a ambiguidade sobre quem efetivamente constituía o "povo" na democracia. Essa complexidade conceitual se revela essencial para entendermos o desenvolvimento da democracia contemporânea.

No decorrer do desenvolvimento histórico da democracia, especialmente com o advento do constitucionalismo, a ideia de "*kratos*" passou a ser também interpretada de diferentes formas, refletindo a distinção entre poder sobre o povo e poder exercido pelo povo. A noção de quem decide, como se decide e o que pode ser decidido tornou-se central na construção das democracias modernas. (AIETA, 2014) ressalta que o constitucionalismo contemporâneo introduz uma multiplicidade de interpretações que tornam o conceito de democracia uma construção política e jurídica contínua, em que

modernidade: poder limitado, dignidade da pessoa humana, direitos fundamentais, justiça material, tolerância, respeito ao outro e – quem sabe? – até felicidade" (2018, p. 288).

o povo é tanto agente quanto destinatário do poder. Nesse sentido, o Estado Democrático de Direito é concebido não apenas como um conjunto de normas, mas como um sistema dinâmico em que os direitos são continuamente atualizados e reinterpretados conforme as demandas da sociedade.

Marilena Chauí complementa essa análise ao destacar que, em uma verdadeira democracia, não basta a simples participação formal do povo nos processos decisórios. Democracia não deve ser compreendida apenas como um regime que permite a eleição periódica de representantes, mas como um sistema que continuamente cria e recria direitos, promovendo a inclusão social e a igualdade. Chauí enfatiza que a criação de novos direitos é o que permite à democracia superar os limites impostos pelas desigualdades estruturais de classe, raça e gênero. Dessa forma, a participação política torna-se não apenas um direito formal, mas uma prática efetiva que transforma as condições sociais, assegurando que a democracia seja um regime em constante evolução.

Carole Pateman também contribui para essa discussão ao abordar a teoria democrática sob o viés da participação. Para Pateman (1992), a essência da democracia reside na participação ativa e significativa dos cidadãos em todos os níveis da vida política. Ela critica as concepções liberais que restringem a participação política ao ato de votar em eleições periódicas, argumentando que a democracia verdadeira só pode ser alcançada quando os cidadãos estão diretamente envolvidos nos processos decisórios cotidianos. A participação política, segundo Pateman, não apenas fortalece a democracia, mas também educa os cidadãos, promovendo um desenvolvimento político e moral contínuo³⁴.

³⁴ Referida discussão se coloca, na contemporaneidade, também no que diz respeito aos conceitos procedimental e epistêmico da democracia. O debate em torno da democracia epistêmica levanta questões fundamentais sobre a relação entre conhecimento, verdade e democracia. A partir da análise das filosofias de John Stuart Mill e William James, Gustavo Hessmann Dalaqua defende a possibilidade de uma concepção epistêmica da democracia que não apenas admite a busca pela verdade no âmbito democrático, mas a considera um aspecto crucial do regime. Contudo, essa defesa não é simples, dado que muitos autores contemporâneos, como Nadia Urbinati, criticam a associação entre democracia e verdade, argumentando que tal aliança tornaria o regime democrático inóspito ao pluralismo, ao dissenso e ao conflito, elementos centrais da democracia moderna. Urbinati, ao subscrever a dicotomia platônica entre *doxa* (opinião) e *episteme* (conhecimento), sustenta que a busca pela verdade pode desvirtuar a política democrática, que deve estar focada no procedimento e na igualdade política dos cidadãos. Para ela, ao buscar a verdade como critério de legitimidade das decisões, a democracia epistêmica corre o risco de transformar-se em uma tecnocracia, onde a competência de poucos superaria o poder decisório da maioria. O receio, segundo Urbinati, é que o enfoque epistêmico deslocaria o critério de julgamento das decisões políticas para fora do processo democrático, abrindo

Tais definições preenchem de ainda mais sentido aquilo que a definição liberal de Norberto Bobbio, em obra já clássica, apresentou para o instituto. Com efeito, o jusfilósofo italiano, ao diferenciar liberalismo e democracia, enfatiza que a democracia, enquanto sistema político, não deve ser reduzida a um conjunto de regras formais ou a um simples mecanismo de escolha de governantes. Para Bobbio, a democracia representa o modo pelo qual o poder é distribuído e controlado, tendo como base fundamental a proteção das liberdades individuais. No entanto, ele distingue a democracia de regimes autocráticos ou totalitários ao sublinhar que a democracia deve operar dentro dos limites de um sistema jurídico que assegure os direitos fundamentais, especialmente as liberdades civis, que são a essência do liberalismo.

espaço para o governo dos sábios, a epistocracia. Nesse sentido, a verdade poderia suprimir o debate e o dissenso, promovendo uma homogeneização que seria antidemocrática. No entanto, Dalaqua, ao revisitar as obras de John Stuart Mill, especialmente *On Liberty* e *Considerations on Representative Government*, propõe uma visão mais complexa da relação entre verdade e democracia. Para Mill, a democracia, ao possibilitar o debate livre e inclusivo, é o melhor regime para promover o conhecimento e a verdade. O filósofo argumenta que a verdade não é algo fixo ou imutável, como no pensamento platônico, mas sim uma construção contínua, que emerge justamente do confronto de ideias e opiniões. Nesse sentido, a verdade democrática é falibilista, ou seja, está sempre sujeita à revisão e ao questionamento. A deliberação pública é essencial para esse processo, pois é no debate entre diferentes perspectivas que se chega a um maior entendimento sobre os problemas sociais. A visão de Mill sobre a verdade como algo mutável e socialmente construído é aprofundada pelo pragmatismo de William James. Para James, a verdade não é uma entidade estática, mas um processo dinâmico, que se transforma à medida que novas experiências e argumentos surgem. Essa concepção pragmatista da verdade está em perfeita sintonia com o regime democrático, que deve ser constantemente revisado e adaptado às novas circunstâncias e desafios. A ideia de que as verdades "políticas" são temporárias e sujeitas a mudanças é central tanto para Mill quanto para James, e contrasta diretamente com a visão tecnocrática ou epistocrática criticada por Urbinati. Dalaqua também aponta que a crítica à democracia epistêmica se baseia na suposição de que a verdade é incompatível com o pluralismo. No entanto, Mill argumenta que o pluralismo é justamente o que possibilita a construção da verdade na política. A diversidade de opiniões e a presença de diferentes grupos sociais no processo deliberativo são essenciais para a criação de uma visão mais ampla e precisa dos problemas enfrentados por uma sociedade. Ao incluir diferentes perspectivas, a democracia representativa permite que as decisões políticas sejam mais sábias e justas, uma vez que levam em conta a multiplicidade de experiências e conhecimentos dos cidadãos. Desse modo, a defesa da democracia epistêmica, tal como elaborada por Dalaqua, reconhece que asserções com pretensão de verdade não podem ser simplesmente banidas do debate democrático. Em certos momentos, é fundamental que questões factuais e asserções verdadeiras sejam levadas em consideração, especialmente quando estão em jogo direitos fundamentais ou políticas públicas que envolvem a saúde, a segurança ou o bem-estar dos cidadãos. Nesse sentido, a democracia epistêmica não deve ser vista como uma ameaça ao dissenso, mas como um modo de enriquecer o debate público, tornando-o mais informado e menos suscetível a erros grosseiros. Por outro lado, Dalaqua também reconhece as limitações dessa concepção. Ele ressalta que, em muitos casos, a deliberação política não visa tanto a descoberta de uma verdade absoluta, mas a criação de um *modus vivendi* entre grupos com visões irreconciliáveis. Nesses momentos, o objetivo da deliberação não é encontrar a verdade, mas garantir a coexistência pacífica entre diferentes interesses e valores. No entanto, mesmo nesses casos, a deliberação democrática desempenha um papel crucial no desenvolvimento moral e intelectual dos cidadãos, ao incentivá-los a reconsiderar suas posições e a enxergar os problemas por outras perspectivas. (DALAQUA, 2017).

Bobbio, no âmbito de “Liberalismo e Democracia” (2017), afirma que um dos maiores desafios das democracias contemporâneas é precisamente a harmonização entre a proteção das liberdades individuais e a ampliação da participação política. Segundo ele, enquanto o liberalismo se concentra na garantia de direitos individuais frente ao poder do Estado, a democracia exige a participação ativa do cidadão na vida política. Esse equilíbrio entre a limitação do poder e a inclusão de novos direitos é o que permite a continuidade e a legitimidade da democracia em uma sociedade pluralista. A criação de direitos, como defendido por Marilena Chauí, encaixa-se justamente nesse contexto, uma vez que a democracia precisa continuamente gerar novos direitos para atender às necessidades emergentes da população, sem perder de vista a garantia das liberdades fundamentais.

Nem só de convergências, porém, vivem as reflexões da filósofa brasileira e do jusfilósofo italiano. Com efeito, Marilena Chauí critica o neoliberalismo como um projeto político que, ao promover a primazia do mercado sobre o Estado, dismantela a capacidade das instituições públicas de promover justiça social e igualdade. Para Chauí, o neoliberalismo transforma a lógica econômica em um princípio organizador de todas as esferas da vida social, inclusive da política, o que resulta na mercantilização dos direitos e na exclusão de grandes parcelas da população do processo democrático. Ao transferir o poder decisório do Estado para o mercado, o neoliberalismo, portanto, não só diminui a ação estatal, mas também enfraquece a capacidade de o Estado agir em prol dos mais vulneráveis, perpetuando e ampliando as desigualdades sociais (2018, p. 420).

Chauí vai além, conceituando o neoliberalismo como um regime totalitário³⁵. Essa definição se dá porque, na visão da autora, o neoliberalismo invade e controla todas as dimensões da vida social, econômica e política, não deixando espaço para alternativas fora da lógica de mercado. Ela afirma que o neoliberalismo não se limita a regular as atividades econômicas, mas impõe seus valores e mecanismos a todas as esferas da sociedade, o que inclui a educação, a saúde, as relações de trabalho e a política. Nesse sentido, a liberdade de escolha e a autonomia dos indivíduos são corroídas pela imposição de um único modelo econômico, que molda o

³⁵ Nesse aspecto, é acompanhada pela definição que o sociólogo polonês Zygmunt Bauman oferece em “Modernidade Líquida” (2001, p. 34).

comportamento humano de acordo com as demandas do capital. Para Chauí, essa submissão de todas as esferas da vida à lógica mercadológica é característica de um sistema totalitário, pois anula o pluralismo, a diversidade de formas de organização social e a capacidade de resistência. O neoliberalismo, segundo a filósofa brasileira, concentra o poder em uma elite econômica, restringe o campo das decisões políticas e exclui a maioria da população dos processos democráticos, mantendo um controle hegemônico que lembra as características de um regime totalitário, onde não há espaço para a divergência ou para a construção de direitos fora da lógica de mercado.

Essa crítica ao neoliberalismo como totalitário está fundamentada na ideia de que o regime neoliberal reduz os cidadãos a consumidores³⁶, limitando suas vidas ao espaço do mercado e subordinando os direitos sociais e políticos às leis da oferta e da procura. Nesse processo, as instituições democráticas são desvirtuadas e instrumentalizadas para atender aos interesses do mercado, não mais como promotoras da justiça social, mas como garantidoras da estabilidade e do lucro econômico. Assim, Chauí argumenta que, ao esvaziar o sentido de participação política e ao desvalorizar a criação de novos direitos, o neoliberalismo compromete os fundamentos da democracia e transforma-se em um sistema que controla, explora e marginaliza, justificando, dessa forma, seu enquadramento como um regime de natureza totalitária.

Por outro lado, Norberto Bobbio, em sua defesa do liberalismo, oferece uma visão distinta. Para Bobbio, o liberalismo é essencial à democracia, pois garante a proteção das liberdades individuais contra o arbítrio do Estado. Ele não se opõe à ideia de Estado, mas defende que o papel fundamental do liberalismo é limitar o poder estatal para proteger os direitos civis e políticos dos indivíduos. Talvez, portanto, a distinção esteja nas nuances apreendidas pelos autores para conceituar *neoliberalismo* e *liberalismo*: o liberalismo de Bobbio não é sinônimo de um mercado desregulado, como o neoliberalismo criticado por Chauí. Em vez disso, ele vê no liberalismo uma ferramenta para assegurar que o Estado não se torne tirânico, preservando um espaço para a autonomia individual e a participação cidadã. Para Bobbio, o equilíbrio entre o poder do Estado e as liberdades individuais é crucial para uma democracia funcional.

³⁶ Nesse aspecto, igualmente Bauman, em "Vida para consumo" (2008, p. 150-151).

O ponto de divergência central entre Chauí e Bobbio está, portanto, no impacto do mercado e do Estado na sociedade. Enquanto Chauí critica o neoliberalismo por subordinar os direitos ao mercado e enfraquecer o Estado como garantidor da igualdade, Bobbio defende que o liberalismo é necessário para proteger os cidadãos de um Estado que, sem limites, poderia violar as liberdades individuais. Para Chauí, o neoliberalismo é uma ameaça direta à democracia porque favorece a concentração de riqueza e poder, enquanto para Bobbio, o liberalismo é um componente essencial para que a democracia exista em um ambiente de respeito às liberdades fundamentais.

Mesmo nesse aspecto, é possível identificar um ponto de convergência entre os dois autores: ambos veem a democracia como um regime que deve continuamente se renovar e adaptar para proteger os direitos dos cidadãos. Chauí defende que a criação de novos direitos é essencial para que a democracia responda às novas demandas sociais, enquanto Bobbio reconhece que a democracia precisa de um equilíbrio entre a expansão da participação e a proteção das liberdades. Em última instância, embora suas ênfases sejam diferentes, ambos concordam que a democracia não pode ser reduzida a um mecanismo formal, mas deve ser um sistema vivo, que protege e amplia os direitos e as liberdades dos cidadãos.

A partir dessas reflexões, fica evidente que o direito à proteção de dados pessoais se insere diretamente na discussão sobre a criação de novos direitos em uma democracia. A crescente digitalização das interações sociais, econômicas e políticas exige a tutela de direitos fundamentais que respondam às realidades contemporâneas, em que a privacidade e o controle sobre as informações pessoais são elementos cruciais para o exercício da autonomia individual. Em um Estado Democrático de Direito, a proteção dos dados pessoais vai além de um mero requisito técnico; ela representa a garantia de que os cidadãos, enquanto povo, não serão explorados ou controlados por corporações ou Estados, que poderiam utilizar esses dados de forma a comprometer direitos fundamentais. Assim como Chauí argumenta que a criação de novos direitos é essencial para superar as desigualdades estruturais e garantir a participação efetiva de todos os cidadãos, a proteção de dados pessoais emerge como uma nova fronteira de direitos, especialmente em um contexto de crescente vigilância digital e de "colonialismo de dados".

A proteção de dados pessoais, no contexto de uma democracia, não é, portanto, apenas uma questão técnica ou jurídica, mas uma necessidade política e social de preservar os fundamentos da liberdade e da autodeterminação dos indivíduos³⁷. A democracia, enquanto regime que garante a participação ativa dos cidadãos nos processos decisórios, depende da existência de um ambiente em que os indivíduos possam exercer suas liberdades sem o risco de vigilância excessiva ou controle indevido. Nesse sentido, a proteção dos dados pessoais está intrinsecamente ligada à manutenção de um espaço público democrático, no qual os cidadãos possam interagir, deliberar e participar politicamente sem receio de que suas informações sejam manipuladas ou utilizadas para fins contrários a seus interesses. A transferência internacional de dados pessoais, quando não regulamentada de maneira eficaz, pode comprometer essas liberdades ao permitir que governos ou corporações estrangeiras colem, analisem e utilizem dados pessoais de forma a influenciar ou controlar o comportamento dos indivíduos, o que constitui uma violação direta dos princípios democráticos de transparência e controle público.

A transferência internacional de dados, quando realizada sem as salvaguardas adequadas, gera um novo tipo de desigualdade entre Estados e cidadãos, uma vez que populações de países menos desenvolvidos ou com marcos regulatórios frágeis se tornam particularmente vulneráveis ao "colonialismo de dados". Isso implica que grandes corporações ou nações mais poderosas podem exercer uma forma de dominação digital sobre indivíduos e nações, minando a soberania democrática e o princípio de igualdade entre os povos. Em um contexto de globalização, a proteção de dados pessoais deve ser vista como um direito que transcende fronteiras, exigindo cooperação internacional para garantir que os cidadãos de todos os países sejam igualmente protegidos, independentemente de onde seus dados são armazenados ou processados³⁸. A criação de marcos regulatórios globais, baseados nos princípios

³⁷ Sobre o princípio da autodeterminação informativa, ver (Mendes; Gico Junior), 2016.

³⁸ Nesse aspecto, Bauman reflete que "poder e política estão se separando. O poder agora existe num espaço global e extraterritorial, mas a política, que antes ligava interesses individuais e públicos, continua local, incapaz de agir em nível planetário. Sem controle político, o poder torna-se fonte de grande incerteza, enquanto a política parece irrelevante para os problemas e temores da vida das pessoas. O poder de vigilância, tal como o exercido por departamentos governamentais, agências de polícia e corporações privadas, enquadra-se muito bem nessa descrição. Até as fronteiras nacionais, antes geograficamente localizadas – ainda que de modo arbitrário –, agora aparecem, nos aeroportos, distantes das "bordas" territoriais, e, o que é mais significativo, em bases de dados que podem nem estar "no" país em questão". (2013, p. 13).

democráticos de transparência, responsabilização e participação, é, portanto, fundamental para assegurar que o controle sobre os dados pessoais permaneça nas mãos dos cidadãos e de seus representantes eleitos, e não nas mãos de corporações ou Estados estrangeiros que não respondem democraticamente às populações afetadas. A proteção de dados, nesse sentido, torna-se uma extensão do direito à participação política, uma vez que garante a capacidade dos indivíduos de exercer controle sobre suas informações em um mundo cada vez mais digital e interconectado.

Além disso, a exploração econômica dos dados pessoais, especialmente por corporações estrangeiras, representa uma nova forma de dominação que reduz o valor intrínseco desses dados ao seu valor de mercado, transformando informações sensíveis em mercadorias a serem compradas e vendidas. Quando empresas multinacionais, predominantemente sediadas em países centrais, se apropriam dos dados pessoais de cidadãos de países periféricos, elas não apenas violam a soberania desses Estados, mas também perpetuam desigualdades globais, impedindo o livre desenvolvimento das nações menos favorecidas. Ao controlar grandes quantidades de dados, essas corporações têm acesso a uma vasta fonte de poder econômico e político, que lhes permite influenciar políticas públicas, mercados e até comportamentos sociais nesses países. A captura e o uso não regulamentados desses dados minam as capacidades internas de desenvolvimento tecnológico e inovação das economias periféricas, uma vez que as próprias informações geradas por seus cidadãos são utilizadas para benefício econômico externo. Esse cenário consolida um novo tipo de dependência digital, onde os países em desenvolvimento ficam reféns de corporações estrangeiras que detêm o monopólio sobre os fluxos de dados, dificultando a autonomia e o crescimento sustentável dessas nações no cenário global.

Nesse contexto, o conceito de *povo* torna-se central na análise de Friedrich Müller (2013), pois ele questiona de maneira crítica quem realmente compõe o "povo" em uma democracia e como essa definição impacta diretamente a legitimidade do poder. Para Müller, a ideia de *povo* é fundamental, uma vez que o "povo" é não apenas o titular do poder constituinte, mas também a fonte última de autoridade em um regime

democrático³⁹; mas esse conceito, historicamente, foi frequentemente restrito e utilizado para justificar a exclusão de determinados grupos da participação política. A composição desse *povo* — quem é incluído ou excluído — determina quem tem o direito de participar das decisões políticas e de influenciar os rumos do Estado, o que, por sua vez, afeta profundamente a legitimidade do exercício do poder em uma democracia.

Nesse aspecto, grupos marginalizados por razões de classe, gênero, etnia ou nacionalidade, muitas vezes, são deixados à margem do que Müller denomina "povo ativo", aqueles que têm o direito de participar diretamente das decisões políticas por meio do voto e da atuação cívica — razão pela qual a análise de Friedrich Müller sobre o conceito de povo traz à tona uma dimensão essencial para a compreensão da democracia contemporânea, que também vai além da estrutura liberal defendida por Bobbio.

Desse modo, Müller problematiza a questão da inclusão e exclusão no seio da democracia, levantando a centralidade da pergunta "quem é o povo?" como um critério fundamental para definir os limites do próprio regime democrático e para compreender como a legitimidade das decisões políticas é conferida. Ao explorar essas diferentes camadas do conceito de povo, Müller se debruça sobre o uso jurídico e político do termo "povo" nas constituições democráticas. Nesse sentido, embora as constituições invistam o povo de poder, como ocorre no preâmbulo da Constituição brasileira de 1988, nem todos os membros da sociedade são, de fato, incluídos como parte ativa desse poder.

Müller identifica, nesse contexto, diferentes dimensões de "povo": o *povo ativo*, que participa diretamente das decisões por meio do voto e da atuação política; o *povo*

³⁹ Nesse sentido concordam autores como Friedrich Müller ("o termo "democracia" não deriva apenas etimologicamente de "povo". Estados democráticos chamam-se governos "do povo" ["*Volks'herrschaften*]; eles se justificam afirmando que em última instância o povo estaria "governando" ["*herrscht*"]. Todas as razões do exercício democrático do poder e da violência, todas as razões da crítica da democracia dependem desse ponto de partida" — 2013, p. 47), José Joaquim Gomes Canotilho ("hoje, o titular do poder constituinte só pode ser o povo, e que o povo, na actualidade, se entende como uma grandeza pluralística formada por indivíduos, associações, grupos, igrejas, comunidades, personalidades, instituições, veiculadores de interesses, ideias, crenças e valores, plurais, convergentes ou conflitantes" — 2007, p. 65-66) e Nicola Matteucci ("o poder constituinte, como poder último, deve se legitimar por meio de sua expressão em um procedimento legal; este fato histórico originário não é justificado apenas pela obediência, mas pelo seu modo de expressão jurídica, modo este cuja formalização garante o poder constituinte do povo [...] Pois a constituição não é um ato de governo, mas um ato do povo" — Matteucci, 1987, p. 892).

como *instância de atribuição*, que confere legitimidade às decisões estatais; o *povo ícone*, que se refere a uma representação simbólica e idealizada do povo, utilizada frequentemente em discursos políticos e constitucionais para legitimar decisões e ações do Estado; e o *povo destinatário*, que recebe as prestações do Estado e os direitos civis e sociais⁴⁰. Em muitas sociedades, especialmente em Estados que se consideram democráticos, o povo ativo é restrito aos cidadãos que possuem direitos eleitorais, o que exclui estrangeiros, menores de idade e outros grupos marginalizados.

Não é demais repisar, nesse contexto, o destaque dado por Müller à exclusão de certos grupos do chamado *povo ativo*, o que restringe a legitimidade democrática. Ele questiona a adequação de regimes democráticos que negam o direito de participação política a segmentos significativos da população, e que compõem o conceito de *povo destinatário das prestações civilizatórias do Estado*⁴¹. Para Müller, essa exclusão cria uma dissonância entre a legitimidade formal do Estado e sua realidade social, enfraquecendo a própria ideia de democracia como autogoverno do povo. Ele também aponta que essa exclusão pode ser manipulada por regimes autoritários que mantêm a aparência de legalidade democrática, mas operam com base na marginalização e na negação de direitos a grupos inteiros.

Nesse cenário, a conexão entre o conceito de *povo destinatário das prestações civilizatórias do Estado* e o direito à proteção de dados pessoais torna-se evidente. O *povo destinatário*, conforme Müller, é aquele que recebe as prestações do Estado, incluindo os direitos civis, sociais e econômicos que visam garantir sua dignidade e igualdade. No contexto atual, em que a informação e os dados pessoais se tornaram

⁴⁰ Análise também contemporânea sobre o tema pode ser encontrada em Aieta (2016).

⁴¹ De forma mais analítica, o conceito de povo destinatário em Friedrich Müller refere-se àquela parcela da população que, embora não participe diretamente das decisões políticas ou da formulação das normas, é a principal receptora das prestações e garantias oferecidas pelo Estado. Esse "povo" inclui todos os indivíduos que são sujeitos de direitos civis, sociais e econômicos, como saúde, educação, seguridade social, e proteção legal, mas que não necessariamente exercem direitos políticos plenos, como o direito ao voto ou a elegibilidade. O povo destinatário é, assim, uma categoria passiva no sentido político, mas ativa no sentido de ser o beneficiário das políticas públicas e da proteção estatal. Müller problematiza que, embora esse "povo" esteja juridicamente incluído como destinatário das ações estatais, ele pode ser politicamente marginalizado, uma vez que não tem influência direta sobre as decisões que definem essas mesmas políticas. Em muitas democracias, há uma dissonância entre a abrangência dos direitos concedidos ao povo destinatário e sua capacidade de participar das deliberações políticas que afetam sua vida cotidiana. Portanto, o conceito de povo destinatário ressalta a importância de incluir todas as camadas da sociedade na formulação e implementação das decisões políticas, para evitar a perpetuação de desigualdades e exclusões estruturais. (2013, p. 70).

ativos fundamentais para a participação plena na sociedade, a proteção de dados pessoais surge como uma dessas prestações essenciais, uma vez que assegura aos indivíduos o controle sobre suas informações e, conseqüentemente, sobre sua autonomia. Assim, garantir o direito à proteção de dados pessoais é uma forma de inclusão democrática, permitindo que o povo destinatário, especialmente os grupos marginalizados, seja devidamente protegido contra abusos, discriminações e exclusões no ambiente digital.

Ao incluir o direito à proteção de dados no rol de prestações constitucionais, o Estado cumpre seu papel de assegurar – ao menos formalmente – que todos os membros da sociedade possam exercer suas liberdades de maneira plena, sem o risco de terem suas informações manipuladas por interesses privados ou estatais que poderiam subverter o equilíbrio democrático. Esse direito se torna, portanto, um elemento vital para a promoção da justiça social, visto que, sem ele, o povo destinatário não tem garantias de participação igualitária nos processos de decisão política, nem de acesso justo aos benefícios de uma sociedade cada vez mais digitalizada. A proteção de dados pessoais, então, se revela essencial para o soerguimento de uma democracia inclusiva e substancialmente legítima.

A teoria de Müller complementa a crítica de Chauí ao neoliberalismo, ao destacar como a restrição da participação política e a mercantilização dos direitos corroem as bases da democracia. Ambos os autores convergem na visão de que a verdadeira democracia só pode existir quando todos os cidadãos são incluídos no processo decisório e quando os direitos são continuamente ampliados para responder às demandas emergentes da sociedade. Assim como Chauí denuncia que o neoliberalismo exclui grande parte da população da vida política e social, Müller expõe as falhas estruturais de democracias que, apesar de suas promessas constitucionais, mantêm práticas excludentes que negam a igualdade plena a todos os cidadãos.

A análise de Müller revela, por fim, que a democracia deve ser constantemente revista e aprimorada para assegurar que o "povo" mencionado nas constituições seja, de fato, uma entidade inclusiva e representativa de toda a sociedade. O conceito de povo, portanto, não pode ser estático ou restritivo, mas deve ser dinâmico e adaptável às mudanças sociais e políticas. Somente por meio de uma inclusão efetiva de todos

os membros da sociedade na esfera política é que a democracia pode realizar seu potencial máximo como regime de liberdade, igualdade e justiça social.

Em síntese, a criação e tutela constitucional efetiva desse novo direito à proteção de dados pessoais reflete a necessidade de adaptação da democracia às transformações tecnológicas, garantindo que o povo, em suas diferentes dimensões, conforme Müller, seja protegido contra abusos que possam ser cometidos no ambiente digital. A tutela efetiva dos dados pessoais envolve assegurar que todos, sem exceção, tenham seus direitos respeitados e possam exercer sua cidadania plena, sem medo de serem monitorados ou terem suas informações exploradas para finalidades que escapam de seu controle. O desafio, portanto, está em criar um marco regulatório que seja sensível às realidades sociais e políticas de um povo cada vez mais dependente das tecnologias, sem perder de vista os princípios democráticos de transparência, participação e responsabilização.

Nesse sentido, a proteção de dados pessoais se alinha à ideia de que a democracia precisa continuamente gerar novos direitos para responder às demandas emergentes da população, tal como Chauí propõe. Ademais, a aplicação desses conceitos à questão da transferência internacional de dados pessoais é fundamental para entender a necessidade de uma proteção efetiva dos cidadãos frente ao “colonialismo de dados” e ao interesse financeiro das corporações. Quando se permite que dados pessoais sejam coletados e explorados por entidades estrangeiras sem controle democrático, o “povo”, enquanto titular do poder constituinte, é excluído de um processo decisório que afeta diretamente seus direitos. Nesse cenário, o povo torna-se alvo de exploração econômica, tendo seus dados transformados em mercadoria, enquanto as corporações lucram sem prestar contas aos cidadãos ou respeitar suas prerrogativas de participação política. Essa apropriação de dados compromete a autonomia dos indivíduos e mina a soberania dos Estados periféricos, que veem seu povo, em suas várias dimensões (ativo e destinatário, principalmente), subordinado a interesses externos. Portanto, a criação de um marco regulatório robusto que limite o controle estrangeiro sobre os dados pessoais não é apenas uma questão técnica, mas uma necessidade democrática que visa proteger a dignidade e os direitos fundamentais do povo, garantindo que o poder político, ainda que no ambiente digital, permaneça nas mãos dos cidadãos e de suas instituições legítimas.

Volvendo às lições de Luís Roberto Barroso, o constitucionalista nos ensina que, entre as conquistas mais relevantes da história recente do Brasil, está a transição de um regime autoritário e violento para um Estado Democrático de Direito, simbolizada pela promulgação da Constituição de 1988. A Carta Magna representa o ponto de inflexão dessa trajetória, consolidando os alicerces para a democracia que se seguiu. Ao longo dos mais de trinta anos de vigência, o Brasil experimentou o seu período mais longo de estabilidade institucional, mesmo em meio a crises severas e eventos traumáticos. Barroso destaca que, desde o fim do regime militar, o país enfrentou desafios substanciais, como os escândalos de corrupção envolvendo o Mensalão, a Operação Lava-Jato, e até duas denúncias criminais contra um presidente em exercício. Além disso, enfrentamos dois *impeachments* presidenciais: o de Fernando Collor, em 1992, que contou com amplo apoio popular, e o de Dilma Rousseff, em 2016, que deixou um legado de polarização política sem precedentes (2018, p. 261-263).

Apesar dessas turbulências, a solidez das instituições brasileiras, amparadas pela Constituição, foi testada e demonstrou resiliência. Barroso vê nisso uma das maiores conquistas do Estado Democrático de Direito: a capacidade de resistir a crises profundas sem retroceder às práticas autoritárias do passado. A Constituição de 1988, ao mesmo tempo que limitou o poder do Estado, preservou o espaço para a soberania popular e garantiu que a transição democrática não fosse apenas um momento isolado, mas um processo contínuo de aperfeiçoamento institucional. Assim, a estabilidade institucional brasileira reflete não apenas a robustez do texto constitucional, mas também o amadurecimento de uma democracia que, mesmo jovem, se provou capaz de enfrentar desafios políticos e sociais de grande envergadura⁴².

Além disso, o mundo atual, caracterizado pela rápida digitalização, transforma profundamente as estruturas sociais, econômicas e políticas, criando um novo ambiente onde a informação e os dados se tornam os principais ativos. Para Barroso, a economia de dados substitui as economias tradicionais baseadas em recursos físicos, como terra e petróleo, e desloca o centro de poder para empresas que

⁴² Sobre aquilo que Barroso nomeia de “a importância decisiva das instituições” enquanto uma das lições do século XX em favor da democracia, ver Barroso (2019).

dominam a coleta e processamento de dados. Isso coloca em evidência a importância de se garantir que as novas tecnologias sejam reguladas de modo a proteger os direitos fundamentais, especialmente a privacidade e a liberdade individual (2019, p. 34).

Essa revolução tecnológica apresenta desafios complexos para a democracia, especialmente no que diz respeito à proteção de dados e à privacidade dos cidadãos. A crescente dependência da tecnologia para a comunicação, trabalho⁴³, lazer e até para as decisões políticas coloca em risco os valores democráticos tradicionais. As plataformas digitais, controladas por um pequeno grupo de empresas gigantes, como *Google*, *Facebook* e *Amazon*, concentraram uma quantidade sem precedentes de poder econômico e político⁴⁴. Esse poder é exercido através da coleta massiva de dados, levantando preocupações sobre o uso indevido dessas informações, bem como sobre a vigilância generalizada e a manipulação de comportamentos sociais e políticos⁴⁵.

Por outro lado, a tecnologia também oferece oportunidades para fortalecer a democracia, se utilizada de maneira correta. O Ministro sugere que a digitalização pode ser uma ferramenta poderosa para aumentar a transparência, facilitar a participação cidadã e melhorar a eficiência dos processos governamentais. Governos digitais podem, por exemplo, utilizar dados para otimizar serviços públicos, combater

⁴³ Nesse aspecto, Barroso enfatiza que as inovações tecnológicas não afetam apenas a economia e o discurso público, mas também a natureza do trabalho e das relações sociais. A automação e a inteligência artificial estão transformando o mercado de trabalho, eliminando empregos tradicionais e criando uma nova classe de trabalhadores "invisíveis", marginalizados pela economia digital. Essa transformação intensifica as desigualdades sociais, já que aqueles que não conseguem se adaptar às novas exigências do mercado de trabalho ficam excluídos, tanto economicamente quanto politicamente. A democracia, nesse contexto, enfrenta o desafio de garantir que a transição tecnológica não agrave ainda mais as divisões sociais e econômicas (2019, p. 35).

⁴⁴ Barroso também alerta para os perigos trazidos pela inteligência artificial (IA), especialmente no que diz respeito à sua capacidade de influenciar decisões humanas e até substituir o julgamento humano em várias esferas da vida social. Ele enfatiza que, enquanto a IA apresenta enormes vantagens, como maior precisão em atividades cirúrgicas e menor taxa de acidentes com carros autônomos, ela também traz riscos significativos. O principal deles é o desaparecimento de empregos e a criação de uma nova classe de excluídos digitais, o que pode agravar ainda mais as desigualdades sociais e enfraquecer as bases da democracia liberal (2019, p. 45).

⁴⁵ A relação entre tecnologia e democracia também envolve a forma como as plataformas digitais influenciam o discurso público e o processo eleitoral. Barroso destaca que as redes sociais e outras ferramentas digitais, ao mesmo tempo que democratizaram o acesso à informação, também se tornaram campos férteis para a disseminação de desinformação, discurso de ódio e campanhas de fake news. Isso cria um dilema ético e jurídico sobre como proteger a liberdade de expressão sem permitir que a manipulação de informações comprometa o funcionamento das democracias liberais. A dificuldade de se encontrar um equilíbrio entre regulação estatal e liberdade de expressão nas plataformas digitais é um dos maiores desafios da era digital. (BARROSO, 2019, p. 51-53).

a corrupção e promover políticas baseadas em evidências. Contudo, para que isso seja efetivo, é necessário que os direitos fundamentais, como a privacidade e o controle sobre os dados pessoais, sejam rigorosamente protegidos.

Um aspecto crucial, ressaltado por Barroso, é a necessidade de uma regulação eficaz da economia de dados, tanto em termos de concorrência quanto de proteção dos direitos individuais. Ele compara a situação atual à era das grandes companhias petrolíferas, quando o poder econômico era concentrado em poucas mãos, e defende que, assim como os reguladores intervieram no passado, agora é necessário um esforço global para controlar o poder dessas grandes corporações de tecnologia. Sem uma regulação adequada, o risco é que uma pequena elite global detenha o controle sobre os dados, o que comprometeria a justiça social e a equidade, pilares fundamentais das democracias contemporâneas.

No campo da privacidade, o constitucionalista aponta que a regulação da proteção de dados pessoais tornou-se um imperativo jurídico no século XXI. A Lei Geral de Proteção de Dados (LGPD) no Brasil, assim como o GDPR na União Europeia, são tentativas de garantir que os cidadãos tenham controle sobre suas informações pessoais em um mundo cada vez mais digital. Esses marcos regulatórios são essenciais para impedir abusos e garantir que a revolução tecnológica beneficie a sociedade como um todo, sem comprometer a autonomia dos indivíduos. A regulação da economia de dados e a proteção da privacidade são, assim, fundamentais para garantir que a tecnologia trabalhe em favor da democracia e não contra ela.

Diante de todo esse diagnóstico, Barroso conclui que a revolução tecnológica não é uma ameaça inevitável à democracia, mas um desafio que requer sabedoria e regulação adequada. A tecnologia tem o potencial de fortalecer a democracia, mas isso só ocorrerá se os direitos fundamentais forem rigorosamente protegidos, se a concentração de poder econômico e político for controlada, e se as desigualdades sociais forem enfrentadas com políticas públicas inovadoras e inclusivas.

No interior desse panorama, a transferência internacional de dados pessoais representa um dos maiores desafios para o Brasil e demais democracias globais na era digital. Em um contexto em que dados são tratados como um dos principais ativos econômicos, sua circulação transnacional exige regulamentações robustas que

assegurem não apenas a privacidade dos cidadãos, mas também a preservação de princípios democráticos fundamentais. No Brasil, a Lei Geral de Proteção de Dados (LGPD) estabeleceu diretrizes claras para a proteção de dados pessoais, mas a questão se torna ainda mais complexa quando envolve a transferência desses dados para outros países, onde as leis e normas de proteção podem ser menos rigorosas ou inexistentes. Nesse cenário, é imperativo que o Brasil adote uma postura firme e vigilante, assegurando que qualquer transferência internacional de dados pessoais seja feita em conformidade com os padrões elevados de proteção estabelecidos em sua legislação.

A responsabilidade do Estado brasileiro, nesse sentido, vai além da simples regulamentação interna. A globalização digital criou um ambiente no qual os dados pessoais podem ser processados em jurisdições com diferentes graus de proteção, expondo os cidadãos a riscos consideráveis. A fim de evitar o que se convencionou chamar de "colonialismo de dados", em que grandes corporações ou Estados estrangeiros se apropriam de dados pessoais de forma indiscriminada, é essencial que o Brasil implemente mecanismos rigorosos de controle e supervisão sobre essas transferências. Isso inclui a exigência de que países destinatários dos dados pessoais brasileiros ofereçam um nível de proteção equivalente ao da LGPD, conforme estipulado pela Autoridade Nacional de Proteção de Dados (ANPD). Além disso, deve-se garantir que as empresas responsáveis por essas transferências estejam plenamente comprometidas com a transparência e a responsabilidade na gestão dos dados.

A importância de uma regulamentação rigorosa da transferência internacional de dados reside na necessidade de preservar a soberania informacional e garantir que os direitos fundamentais dos cidadãos brasileiros não sejam comprometidos em um cenário de exploração digital global. O Brasil, ao tutelar esses direitos com responsabilidade, reforça a proteção da democracia ao impedir que dados pessoais sejam usados para manipular processos democráticos, violar a privacidade ou exercer controle econômico e político sobre sua população. A construção de uma regulação sólida e abrangente para a transferência de dados é, portanto, uma peça essencial para o fortalecimento da democracia em tempos de avanço tecnológico.

2.2 O papel crucial da proteção de dados pessoais como princípio constitucional democrático

O entrelaçamento entre uma efetiva proteção dos dados pessoais e os valores subjacentes à democracia vem sendo cada vez mais expostos e estudados por teóricos do direito. Essa foi, sem dúvida, uma das grandes preocupações de Danilo Doneda⁴⁶, desde o início de seu despontar como jurista proeminente, momento em que já salientava sua índole de democrata visceral. Desde sua obra inaugural, a conhecida *Da privacidade à proteção de dados pessoais* (Doneda, 2006) – até hoje tida como um dos mais importantes referenciais de tantos trabalhos acadêmicos – até suas produções mais recentes, em uma vasta quantidade de artigos, se preocupou com temas atinentes à democracia, não olvidando, e mais do que isso, enaltecendo a íntima relação de uma tutela efetiva dos dados pessoais e uma vivência e cultivo efetivos e salutares dos valores democráticos⁴⁷.

Com efeito, logo na introdução de sua obra, Doneda (2020), alerta para a essencial sociabilidade das questões que envolvem a proteção dos dados pessoais, bem como os impactos que as mais atuais tecnologias têm o condão de causar para a fruição de direitos, e mesmo para a estabilidade dos arranjos sociais, que se dão,

⁴⁶ Danilo Doneda é uma referência no campo da proteção de dados pessoais e dedicou grande parte de sua carreira acadêmica e profissional a essa área. Com sua vasta experiência, tanto no setor público quanto no setor privado, adquiriu uma visão abrangente sobre os desafios e oportunidades da proteção de dados pessoais. Doneda também é reconhecido internacionalmente, participou ativamente de debates e conferências em diversos países, momentos em que compartilhou seu conhecimento e experiência com especialistas de diferentes origens, engendrando, não raras vezes, artigos e escritos em parceria com importantes pensadores de diversas nacionalidades, publicados na Europa, Estados Unidos e América Latina.

⁴⁷ Na obra inaugural do Professor Doneda, referências à palavra “democracia” e suas variações - democrático(s), democrática(s), democratizaram, democratização, *et al* – aparecem, ao longo do texto, 22 (vinte e duas) vezes. Ora, é claro que a mera presença dos vernáculos nada revelam sobre as ideias do autor acerca de seus conteúdos. Com efeito, sua interpretação sobre a democracia e seus valores subjacentes poderia ser, ante o que admite a contingência da sensibilidade, negativa. E a interpretação no Direito é condição de sua própria expressão, naquilo que comumente se alcunha de “reconstrução” de sentido a partir do texto normativo, assentada na premissa de que “não há correspondência biunívoca entre dispositivo e norma – isto é, onde houver um não terá obrigatoriamente de haver o outro” (ÁVILA, 2016, p. 51). Não é da quantidade de vezes em que presentes referidos termos nos textos do autor, portanto, que se extrai senão uma firma aderência à democracia, mas a razão pela qual apareceram, ou seja, o contexto no qual foram invocados, e a que tipo de contextos e significados foram atrelados.

no mais das vezes, na realidade ocidental, mediante e sob a salvaguarda de um escorreito funcionamento de sistemas democráticos⁴⁸.

Ao situar essa referência inicial à democracia, Doneda⁴⁹ aponta que a proteção de dados pessoais não se limita à salvaguarda da privacidade. O objetivo é, na verdade, assegurar uma proteção ampla da pessoa, defendendo-a contra diferentes formas de controle e discriminação, a fim de preservar aspectos essenciais de sua liberdade pessoal. Além disso, a questão já não afeta apenas o indivíduo isoladamente – como tradicionalmente se entendia no direito à privacidade –, mas alcança também diferentes coletividades. Por fim, ao contextualizar essa primeira menção à democracia, Doneda indica que referidas reflexões, ao fazerem referência, a um, ao balanço de poderes no sistema democrático, e, a dois, ao combate à discriminação e defesa de grupos sociais vulneráveis, vão ao encontro do que prescrevem o art. 2º⁵⁰, 3º, I, III e IV⁵¹, e 5º, XLI⁵², todos da Constituição Federal.

Ao avançar na leitura da obra, se verifica que tal concepção é reforçada por Doneda⁵³. Ao abordar a questão da privacidade, agora consagrada como um direito fundamental, e confrontá-la com os traços individualistas de sua origem, destaca que essas mesmas relações, intensificadas pela expansão do fluxo de informações pessoais, revelaram um novo aspecto da própria privacidade: sua relevância como

⁴⁸ Indica o autor que: O problema da proteção de dados, mais do que uma questão individual, possui implicações sociais profundas, que vão desde questões atinentes ao gozo de direitos por coletividades até a viabilidade de modelos de negócio que podem ser intrinsecamente contraditórios com o efetivo controle dos próprios dados pessoais, e mesmo o balanço de poderes no sistema democrático. (DONEDA, 2020, p. 27)

⁴⁹ No original: na proteção de dados pessoais não é somente a privacidade que se pretende tutelar, porém busca-se a efetiva tutela da pessoa em vista de variadas formas de controle e contra a discriminação, com o fim de garantir a integridade de aspectos fundamentais de sua própria liberdade pessoal. E, ainda, não é mais somente o indivíduo a ser o único afetado – um antigo paradigma do direito à privacidade –, porém inteiras classes e grupos sociais (*Idem*).

⁵⁰ São Poderes da União, independentes e harmônicos entre si, o Legislativo, o Executivo e o Judiciário.

⁵¹ Art. 3º Constituem objetivos fundamentais da República Federativa do Brasil:

I - construir uma sociedade livre, justa e solidária;

(...)

III - erradicar a pobreza e a marginalização e reduzir as desigualdades sociais e regionais;

IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação.

⁵² Art. 5º (...)

(...)

XLI - a lei punirá qualquer discriminação atentatória dos direitos e liberdades fundamentais;

⁵³ No original: “foram essas mesmas relações, potencializadas pelo crescimento do fluxo de informações pessoais, que lançaram luz sobre um outro aspecto da privacidade: a sua importância para uma sociedade democrática como pré-requisito fundamental para o exercício de diversas outras liberdades fundamentais” (DONEDA, 2020, p. 32).

base essencial para o exercício de várias liberdades fundamentais em uma sociedade democrática (DONEDA, 2020, p. 32).

O processo de convergência do ordenamento em torno da pessoa humana, particularmente acelerado e moldado pelas condições específicas do período correspondente à passagem do séc. XIX para o XX, em um processo de mudança na cultura jurídica em uma época na qual a figura da personalidade humana ainda possuía caráter quase que meramente instrumental para o direito, impulsionou o desenvolvimento da ideia de estado social, no qual o ordenamento jurídico assume as funções de estabelecer e promover uma hierarquia de valores, privilegiando a pessoa humana. Tal concepção foi cristalizada, em diversos países, através de uma Constituição, que deixa de ser um instrumento de cunho basicamente político para tornar-se o ponto de convergência de todo o ordenamento – e, com isso, deixando de lado a pretensão de constituir-se em um sistema neutro⁵⁴. Diante dessa realidade é que afirma Doneda que a tarefa dela decorrente “incluía a adequação do instrumental jurídico a uma sociedade democrática com novas características, fruto do início de uma experiência de inclusão social” (DONEDA, 2020, p. 59).

Vê-se, portanto, que a análise de Danilo Doneda sobre a interseção entre a proteção de dados pessoais e os valores democráticos revela uma compreensão profunda de como esse direito transcende a mera questão da privacidade individual, alcançando a defesa da autonomia e da liberdade de toda a coletividade. Ao destacar o papel central que a proteção de dados desempenha no equilíbrio do poder em uma sociedade democrática, o jurista reforça a importância de uma regulação robusta e eficiente que assegure a dignidade da pessoa humana frente às novas tecnologias e ao controle informacional. Nesse sentido, é possível afirmar que a proteção de dados pessoais constitui não apenas uma garantia contra abusos, mas um verdadeiro pilar para a preservação e fortalecimento das democracias modernas.

A par desses aspectos, uma das contribuições mais importantes de Danilo Doneda para o estudo da proteção de dados pessoais é sua defesa enquanto direito

⁵⁴ Não por outro motivo é que, mais adiante, passa a sustentar que a privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento indutor da autonomia, da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Nesse papel, ela é pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos (DONEDA, 2020, p. 93).

fundamental⁵⁵. Ele argumenta que a proteção de dados pessoais é essencial para a dignidade humana e para o pleno exercício da liberdade individual, sendo um sustentáculo fundamental da democracia. Doneda tem destacado a importância de uma abordagem equilibrada na proteção de dados, que leve em consideração não apenas a segurança, mas também os direitos e liberdades dos indivíduos⁵⁶.

No artigo "Novas faces do poder no mundo digital" (DONEDA, 2017), explora o impacto das tecnologias digitais e da internet na reconfiguração das relações de poder. Nesse aspecto, Doneda ressalta como a coleta e o uso de dados pessoais se tornaram ferramentas fundamentais para o exercício de poder, tanto por parte de corporações quanto de Estados, destacando que o controle sobre os dados pessoais pode impactar diretamente a autonomia e liberdade dos indivíduos. A proteção de dados, nesse contexto, emerge como uma necessidade fundamental para garantir que o uso dessas informações não comprometa direitos individuais, tornando-se, assim, uma nova fronteira de direitos fundamentais na era digital.

Em "Proteção de dados pessoais enquanto direito fundamental - privacidade e *e-health*" (2015), Doneda argumenta que a proteção de dados pessoais deve ser vista como um direito fundamental em razão do papel central que a privacidade desempenha no exercício de outras liberdades e direitos fundamentais, como a liberdade de expressão e o direito à saúde. No contexto de saúde eletrônica (*e-health*), a privacidade e a proteção de dados são essenciais para garantir que informações sensíveis dos pacientes sejam protegidas e utilizadas de maneira responsável. Nesse sentido, a proteção dos dados pessoais não é apenas uma questão técnica, mas um imperativo ético e jurídico para a preservação da dignidade e da autonomia dos cidadãos.

⁵⁵ Assim o fez em trabalhos como: Direitos fundamentais e sociedade tecnológica (2022), Tutela jurídica do corpo eletrônico: Novos Desafios ao Direito Digital (2022); STF reconhece o direito fundamental à proteção de dados (2020); Proteção de dados pessoais enquanto direito fundamental e o direito fundamental à saúde – privacidade e *e-Health* (2015), entre outros.

⁵⁶ Em tempos recentes, Doneda contribuiu sobremaneira para a defesa dos brasileiros, ao atuar em Ação Direito de Inconstitucionalidade que questionava a legitimidade de órgãos e de entidades da administração pública federal compartilharem dados pessoais entre si. Em sua sustentação oral no julgamento da ADI 6389, sobre a inconstitucionalidade do art. 2º, caput e §§ 1º e 3º da MP 954/2020 – medida provisória que obrigava a disponibilização de dados pessoais dos usuários de operadoras de telefonia fixa e móvel com o instituto brasileiro de Geografia e estatística (IBGE) – argumentou, com brilhantismo, que o caso dizia respeito não somente a pesquisas realizadas pelo IBGE, mas sobre os próprios parâmetros constitucionais da proteção de dados no Brasil e, ao final, ao valor e significado dos dados pessoais dos brasileiros para a nossa liberdade, personalidade e democracia (2020).

No escrito "Reflexões sobre proteção de dados pessoais em redes sociais" (2012), por sua vez, Doneda discute o impacto das redes sociais na privacidade dos usuários e no tratamento de seus dados pessoais. O jurista curitibano destaca que, no ambiente das redes sociais, a exposição de dados pessoais é intensificada e, muitas vezes, comercializada sem o devido conhecimento ou consentimento dos usuários. Nesse sentido, a proteção de dados pessoais deve ser encarada como um direito fundamental que visa resguardar os indivíduos de práticas abusivas e garantir que eles tenham controle sobre suas informações pessoais. A falta de transparência e o uso indevido de dados reforçam a necessidade de uma regulamentação robusta e de direitos claros para os usuários.

Por fim, em "Risco e Informação Pessoal: o Princípio da Finalidade e a proteção de dados no ordenamento brasileiro" (2010), Doneda analisa o princípio da finalidade, que estabelece que os dados pessoais só podem ser utilizados para os fins para os quais foram coletados, assegurando que as informações não sejam usadas de maneira arbitrária ou para fins que o indivíduo não tenha autorizado. Ele enfatiza que a proteção de dados no Brasil precisa garantir que esse princípio seja rigorosamente aplicado, para que os dados pessoais dos cidadãos não sejam usados de forma que comprometa sua privacidade e segurança. A aplicação desse princípio é fundamental para proteger os cidadãos contra o uso abusivo de suas informações, especialmente em um contexto de crescente digitalização e vigilância.

As diversas reflexões de Danilo Doneda convergem, portanto, para uma visão consolidada da proteção de dados pessoais como um direito fundamental essencial ao Estado Democrático de Direito. Doneda sustenta que a privacidade, entendida como um direito individual e coletivo, é crucial para a manutenção da liberdade e autonomia dos cidadãos em uma sociedade democrática. A proteção de dados pessoais, nesse sentido, não se limita à privacidade individual, mas abrange a defesa contra o controle indevido e a discriminação, garantindo que os cidadãos possam exercer suas liberdades fundamentais sem interferências externas, especialmente no contexto do uso e manipulação de informações pessoais por corporações e Estados.

Além disso, Doneda aponta que, em um mundo digital cada vez mais interconectado, onde o fluxo de informações pessoais está em constante expansão, a proteção de dados pessoais emerge como um direito pré-requisito para o exercício

de outros direitos fundamentais, como a liberdade de expressão, a autodeterminação informativa e a participação política. Nesse contexto, a privacidade torna-se um amparo essencial para a preservação da dignidade humana, fundamental para assegurar que os cidadãos tenham controle sobre suas informações e possam atuar em uma sociedade que valoriza a transparência e a justiça social.

Ao relacionar a proteção de dados pessoais com a estabilidade e o fortalecimento das instituições democráticas, o civilista enfatiza que uma democracia moderna não pode funcionar plenamente sem garantir que os dados pessoais de seus cidadãos sejam tutelados de forma efetiva e ética. A exploração indevida de dados e a falta de transparência nas práticas de tratamento de informações podem comprometer a própria legitimidade do poder democrático, gerando desigualdades e distorções que afetam a participação cidadã e a proteção dos grupos mais vulneráveis.

Além disso, Danilo Doneda se dedicou a analisar os desafios éticos e jurídicos relacionados à proteção de dados em um contexto democrático. Ele enfatiza a necessidade de uma legislação clara e eficaz, que estabeleça diretrizes claras para a coleta, o armazenamento e o uso de dados pessoais⁵⁷. Doneda argumenta que a proteção de dados não deve ser vista apenas como uma preocupação técnica, mas como uma questão que afeta diretamente a relação entre o Estado, as empresas e os cidadãos⁵⁸.

Os anos de defesa de Danilo Doneda, e de outros juristas⁵⁹, em favor do reconhecimento da proteção de dados pessoais como um direito fundamental⁶⁰,

⁵⁷ Uma das áreas em que o trabalho de Danilo Doneda tem sido fundamental, e continuará sendo de suma importância, é na elaboração e implementação da Lei Geral de Proteção de Dados (LGPD) no Brasil. Como um dos principais especialistas no assunto, ele contribuiu para a formulação da lei e tem sido uma voz ativa na promoção de sua implementação adequada. Doneda destaca a importância de uma cultura de proteção de dados na sociedade brasileira, envolvendo a conscientização e a educação de todos os envolvidos, desde as instituições governamentais até as empresas e os cidadãos. Nesse aspecto, destaca-se o trabalho *Experimentações em cultura, educação e cidadania: o caso da Associação Grãos de Luz e Griô* (2009).

⁵⁸ Trabalhos que podem ser citados nessa senda são: *Proteção de Dados na América Latina: Covid-19, Democracia, Inovação e Regulação* (2021); *Inteligência Artificial, Ética e Epistemologia: o Encontro da Tecnologia com as Ciências Sociais* (2021); *Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados* (2019); "Onde eles estavam na hora do crime?": *Ilegalidades no tratamento de dados pessoais na monitoração eletrônica* (2019), entre outros.

⁵⁹ Como exemplo: SARLET, 2020b; MENDES, 2013.

⁶⁰ Em momento pretérito, o Supremo Tribunal Federal havia reconhecido a proteção de dados pessoais como um direito fundamental, no julgamento da Medida Provisória 954/2020, em decisão que não

encontraram eco no poder legislativo brasileiro em 2022. A Proposta de Emenda à Constituição (PEC) nº 17/2019, que culminou na Emenda Constitucional nº 115/2022, consolidou a proteção de dados pessoais como um direito fundamental no artigo 5º da Constituição Federal. A PEC, originada no Senado Federal, propôs a inclusão desse direito entre os direitos e garantias fundamentais e estabeleceu a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais⁶¹.

A justificativa da PEC enfatizou a evolução histórica e a necessidade de proteção jurídica dos dados pessoais em uma era marcada pela digitalização e pelo crescente risco às liberdades individuais. O avanço das tecnologias digitais trouxe novas oportunidades econômicas, mas também expôs cidadãos a possíveis violações de privacidade e manipulação de informações, destacando a necessidade de um regime jurídico claro e centralizado para regular essa questão.

Ao longo de sua tramitação, a proposta recebeu, em diferentes audiências públicas, o apoio de especialistas – entre os quais, de Danilo Doneda – e de membros da sociedade civil, que destacaram que a proteção de dados não se limita à privacidade individual, mas envolve também uma dimensão coletiva e sistêmica, necessária para a estabilidade das democracias modernas. A centralização da competência legislativa na União foi vista como essencial para evitar fragmentação normativa e garantir segurança jurídica, facilitando, assim, o livre fluxo de dados em um ambiente regulatório coeso.

A Emenda Constitucional nº 115/2022, ao formalizar a proteção de dados pessoais como um direito fundamental, também reforçou a necessidade de um marco regulatório robusto que equilibre o avanço tecnológico com a preservação de direitos

apenas suspendeu a eficácia de uma medida que permitia o compartilhamento massivo de dados sem garantias adequadas, mas também firmou um entendimento constitucional sobre a importância da proteção de dados em um contexto de crescente digitalização. Em interessante artigo publicado à época, Laura Schertel Mendes analisou os desdobramentos dessa decisão para a jurisprudência brasileira, apontando que o reconhecimento desse direito pelo STF consolidava a proteção de dados como um pilar da democracia e da proteção dos direitos fundamentais no Brasil. Argumentava, ainda, que a decisão do STF estabelecia um precedente crucial, fortalecendo a posição do Brasil no cenário internacional e assegurando que a proteção de dados seja tratada como uma prioridade constitucional, fundamental para a preservação da dignidade e da autonomia dos cidadãos. Nesse sentido MENDES, 2013..

⁶¹Disponível

em:

<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757#:~:text=PEC%2017%2F2019%20Inteiro%20teor,Proposta%20de%20Emenda%20%C3%A0%20Constitui%C3%A7%C3%A3o&text=Alter%20a%20Constitui%C3%A7%C3%A3o%20Federal%20para,e%20tratamento%20de%20dados%20pessoais>. Acesso em: 02 jan. 2024.

fundamentais. Essa inclusão reflete um compromisso do Estado brasileiro com a proteção dos cidadãos em um contexto digital cada vez mais complexo, onde a coleta e o uso de dados podem impactar diretamente a autonomia e a dignidade das pessoas.

As consequências da positivação do direito à proteção de dados pessoais entre os direitos e garantias fundamentais previstos pelo art. 5º da Constituição Federal foram exploradas, com profundidade e maestria, pelo constitucionalista Ingo Wolfgang Sarlet, em artigo publicado no ano de 2022⁶². Neste trabalho, o autor realiza uma análise minuciosa sobre a promulgação da Emenda Constitucional nº 115/2022, e inicia destacando que, apesar de a proteção de dados pessoais já ser considerada um direito implícito no Brasil, sua inclusão explícita na Constituição carrega uma carga positiva adicional, atribuindo um valor substancial à sua consolidação. Aponta, nesse contexto, que o direito à proteção de dados pessoais é agora reconhecido formalmente como autônomo, com um âmbito de proteção próprio, o que garante ao tema um status jurídico de primeira ordem⁶³, equivalente a outros direitos fundamentais já consagrados no texto constitucional (2022, n.p.).

A inserção do inciso LXXIX ao artigo 5º da Constituição⁶⁴ estabelece a proteção de dados pessoais como direito fundamental, "inclusive nos meios digitais", o que, para Sarlet, não apenas preenche uma lacuna no sistema jurídico brasileiro, mas também fortalece a aplicabilidade imediata desse direito. Ele enfatiza que o reconhecimento expresso deste direito implica que ele assume o regime jurídico-constitucional típico de um direito fundamental, incluindo sua condição de limite

⁶²Disponível em: <https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protacao-dados-pessoais-direito-fundamental/#:~:text=De%20acordo%20com%20o%20texto,n%C2%BA%20115%2C%20de%202022>). Acesso em: 03 jan. 2024.

⁶³ Ao serem incluídos na Constituição, os direitos fundamentais, incluindo o direito à proteção de dados pessoais, passam a ocupar uma posição de superioridade em relação a todo o restante do ordenamento jurídico. Isso significa que qualquer lei ou ato normativo que viole esse direito será considerado inconstitucional. A inclusão da proteção de dados na Constituição reforça a hierarquia desse direito, vinculando todos os outros diplomas legais a seus princípios, e assegura que não pode ser relativizado ou restringido por normas infraconstitucionais, exceto nos limites estritos previstos pela própria Constituição.

⁶⁴ Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[...]

LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022).

material às reformas constitucionais. Dessa forma, o legislador não pode mais suprimir ou modificar este direito sem observar os limites impostos pelo próprio texto constitucional⁶⁵, reforçando sua relevância no contexto do ordenamento jurídico nacional.

Outro aspecto de especial relevância indicado pelo constitucionalista repousa no fato de que, ao ser considerado um direito fundamental, o direito à proteção de dados adquire aplicabilidade imediata, conforme o artigo 5º, § 1º, da Constituição. Isso significa que ele é autoaplicável e não depende de regulamentação infraconstitucional para ser exercido, obrigando tanto o Estado quanto os particulares a respeitar esse direito. Além disso, a inclusão de atores privados na vinculação a esse direito sublinha a sua dimensão horizontal, ou seja, a obrigação de empresas e entidades do setor privado de aderirem aos princípios da proteção de dados, mesmo na ausência de regulamentação específica.

A Emenda Constitucional 115/22 também introduziu, conforme Sarlet, uma reserva legal simples, que outorga ao legislador infraconstitucional a competência para estabelecer restrições ao direito à proteção de dados pessoais. No entanto, essas restrições devem observar os critérios estabelecidos pela Constituição, sob pena de inconstitucionalidade. Isso implica que qualquer intervenção legislativa deve ser rigorosamente fundamentada e proporcional, visando a proteger outros interesses constitucionais de igual peso, como a segurança nacional ou a ordem pública, sem, contudo, violar a essência do direito fundamental.

Outro ponto relevante por ele levantado é a relação da proteção de dados pessoais com outros direitos fundamentais, especialmente a dignidade da pessoa humana e o livre desenvolvimento da personalidade. Argumenta, nesse contexto, que a proteção de dados pessoais está profundamente interligada com esses princípios, pois garante que os indivíduos possam exercer seu direito à autodeterminação informativa, controlando como suas informações são coletadas e utilizadas. O constitucionalista também menciona que essa proteção é essencial para preservar a

⁶⁵ O direito fundamental à proteção de dados assume uma dimensão especial no tocante às emendas constitucionais, tornando-se cláusula pétrea, o que implica que esse direito não pode ser abolido ou modificado substancialmente nem mesmo por emenda à Constituição. Os limites materiais impostos pelo artigo 60, §§ 1º a 4º, da Constituição Federal garantem que esse direito não seja suprimido ou alterado de forma a violar os direitos fundamentais.

liberdade individual em uma sociedade cada vez mais digitalizada, onde o fluxo de informações pessoais é crescente e as ameaças à privacidade são constantes.

O autor também explora o impacto da Lei Geral de Proteção de Dados (LGPD) no contexto da EC 115/2022. Sarlet reconhece que, embora a LGPD tenha sido um grande avanço na regulação do tratamento de dados pessoais no Brasil, sua aplicação carecia de um respaldo constitucional explícito que garantisse uma base sólida para o exercício e a proteção desses direitos. A emenda constitucional, segundo Sarlet, oferece esse respaldo, fortalecendo a LGPD ao vinculá-la diretamente ao texto constitucional, o que impõe novas obrigações ao Estado e às entidades privadas no tratamento de dados pessoais.

Esta figura, inclusive, como uma das questões mais complexas com relação ao direito à proteção de dados pessoais: a presença de lacunas regulatórias, especialmente no que diz respeito à segurança pública, segurança nacional e investigações criminais, áreas que, em grande parte, não são abrangidas pela Lei Geral de Proteção de Dados (LGPD). Com a elevação da proteção de dados à categoria de direito fundamental, o Brasil garante que mesmo nessas áreas sensíveis, onde anteriormente havia uma "zona livre" de proteção, os direitos fundamentais dos cidadãos sejam respeitados, promovendo um equilíbrio entre as necessidades do Estado e a proteção da privacidade individual. Isso implica um dever contínuo de adaptação e regulamentação por parte do legislador, que deve se pautar pelos princípios constitucionais, a fim de evitar que a ausência de regras específicas para esses setores vulnerabilize os direitos dos cidadãos.

Além disso, Sarlet destaca a importância do diálogo entre a legislação nacional e os tratados internacionais de direitos humanos ratificados pelo Brasil, como a Convenção Americana de Direitos Humanos e o Pacto Internacional de Direitos Civis e Políticos. Nesse meandro é que o autor faz uma reflexão sobre o constitucionalismo de múltiplos níveis, que considera essencial para a interpretação e aplicação do direito à proteção de dados pessoais. Esse conceito refere-se à interação entre os níveis nacional, regional e internacional de proteção de direitos humanos, o que, no caso da proteção de dados, envolve o diálogo entre a Constituição brasileira, a LGPD e os tratados internacionais. Em razão disso, argumenta que o direito fundamental à proteção de dados pessoais deve ser interpretado em consonância com esses

tratados, já que o Brasil atribui hierarquia supralegal aos tratados de direitos humanos. Isso implica que o marco normativo infraconstitucional, como a LGPD, deve estar em conformidade tanto com a Constituição quanto com os parâmetros internacionais, reforçando a proteção dos cidadãos contra violações de seus dados pessoais, e garantindo, assim, uma proteção mais robusta e eficaz dos direitos fundamentais, especialmente em um contexto globalizado em que o fluxo de dados pessoais ultrapassa as fronteiras nacionais.

Diante de todos esses conceitos, a conclusão do constitucionalista gaúcho é que a EC nº 115/2022 representa um marco histórico na consolidação do direito à proteção de dados pessoais no Brasil, ao estabelecer uma base sólida para sua aplicação e garantir que esse direito receba a devida importância dentro do ordenamento jurídico. Contudo, ele adverte que a simples positivação do direito na Constituição não basta por si só; é imprescindível que tanto o Estado quanto a sociedade civil permaneçam vigilantes e atuem de maneira proativa para assegurar que a proteção de dados se concretize na prática, e não se limite a uma norma formal inscrita no texto constitucional.

2.3 A tropicalização do pensamento sobre a proteção de dados pessoais

É inegável o interesse brasileiro na tutela dos dados pessoais, já que sua proteção se posiciona com corolário do princípio da dignidade da pessoa humana⁶⁶; além disso, consoante sobredito, desde o mês de fevereiro de 2022, após a promulgação da Emenda Constitucional nº 115/2022⁶⁷, *é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais* – ou seja, o direito à proteção dos dados pessoais é explicitamente contado entre os direitos e

⁶⁶ A própria potencialidade dos meios informáticos para a publicidade e propagação de informações privadas é objeto de análise pelos constitucionalistas, conforme se observa da reflexão feita por José Afonso da Silva, ao lecionar que: *O intenso desenvolvimento de complexa rede de fichários eletrônicos, especialmente sobre dados pessoais, constitui poderosa ameaça à privacidade das pessoas. O amplo sistema de informações computadorizadas gera um processo de esquadramento das pessoas, que ficam com sua individualidade inteiramente devassada. O perigo é tão maior quanto mais a utilização da informática facilita a interconexão dos fichários com a possibilidade de formar grandes bancos de dados que desvendem a vida dos indivíduos, sem sua autorização e até sem seu conhecimento.* (SILVA, 2011. p. 212).

⁶⁷ Ainda que hoje seja contado explicitamente entre os direitos e garantias fundamentais constitucionalmente protegidos, há tempos se defendia, pela melhor doutrina nacional, sua definição enquanto direito e garantia individual *implícita*, nos termos do art. 5º, IV, X, XII e §2º, todos da Constituição da República Federativa do Brasil.

garantias fundamentais dispostos no art. 5º da Constituição da República Federativa do Brasil⁶⁸.

No entanto, ainda que explicitamente se reconheça a estatura constitucional do direito que se pretende tutelar com a LGPD, evidente se mostra que a exigência europeia de um nível de proteção adequado para a transferência legítima de dados pessoais foi o verdadeiro propulsor da promulgação da lei brasileira, conforme se verifica, extensamente, do voto do então relator do PL – apresentado em 24 de maio de 2018, ou seja, *um dia antes* do início da eficácia do Regulamento europeu⁶⁹.

Essa questão não seria de grande relevância se não fossem evidentes, em virtude da atual estrutura econômico-política global, as amplas e significativas implicações associadas à coleta e ao processamento de dados pessoais.

O Estado e os cidadãos brasileiros não gozam de privilégios quando se trata de ataque aos dados pessoais pelos mais diversos entes públicos e privados, sofrendo também as consequências vislumbradas em diversos países ao redor do globo; mais do que isso, ao gozar pouco das vantagens dos polos produtores de tecnologia – porquanto dela consumidor, atuando muito mais como exportador de *commodities* – ocupa, no mais das vezes, não a posição de predador, mas de presa nos palco econômico-globalizado e nos nichos do poder⁷⁰.

Essa posição é reforçada, atualmente, justamente porque as *commodities* mais desejadas pelas empresas mais importantes do planeta são, justamente, os dados pessoais dos habitantes dos mais diversos lugares do mundo.

Exemplos dessa condição de caça buscada pelos predadores tecnológicos mundiais não faltam. O primeiro indicativo comprobatório dessa afirmativa sobre o Brasil advém dos dados consignados no livro escrito por Glenn Greenwald (2014), através dos documentos levados à público por Edward Snowden, vez que, além de exporem números vultosos, relacionam, alguns, especificamente ao país. Nesse sentido, Greenwald relatou que o programa *Boundless Informant* coletou, entre e-

⁶⁸ O amparo constitucional do direito à proteção de dados era, há tempos, preconizado explicitamente por Danilo Doneda, ao afirmar que “a Constituição Federal de 1988 ocupou-se do assunto e incluiu, entre as garantias e direitos fundamentais de seu artigo 5º, a proteção da ‘intimidade’ e da ‘vida privada’ (inciso X), deixando claro que a proteção da pessoa humana abrange estes aspectos”. (DONEDA, 2006, p. 107-108).

⁶⁹ Ver capítulo 3 da tese.

⁷⁰ Tema do capítulo 2.

mails e chamadas telefônicas, em um único período de trinta dias, 2,3 bilhões de registros advindos do Brasil, na forma de metadados⁷¹. Além desse, o programa *Blarney* – voltado a obtenção de parcerias com empresas que permitam o acesso a, principalmente, cabos de fibra ótica – também é relatado como tendo o Brasil como um de seus países alvo⁷².

Greenwald ainda relata que, aliado ao programa de espionagem estadunidense capitaneado, principalmente, pela NSA, encontrava-se o Canadá, e que este se vangloriava, na Conferência de Desenvolvimento de Sinais de 2012, de, por meio de sua Organização de Serviços de Comunicações, ter espionado o Ministério de Minas e Energia do Brasil, agência responsável por regulamentar o setor de maior interesse para as empresas canadenses⁷³.

Por fim, indica que o Brasil figurava entre os países que, com frequência, se tornaram alvos, mas nunca parceiros, dos programas de espionagem dos Estados Unidos, ainda que fosse considerado como uma nação “amigável” ou “neutra”, e não “adversária”, a exemplo da Rússia e da China⁷⁴.

Ao lado das revelações proporcionadas por Edward Snowden, documentos vazados pela organização *WikiLeaks* demonstraram que políticos de alto escalão do governo brasileiro foram alvo de grampos telefônicos pelo governo dos Estados Unidos da América, incluindo a ex-Presidente Dilma Rousseff e o ministro-chefe do Gabinete de Segurança Institucional, General José Elito Siqueira, responsável pela segurança da ex-presidente da República⁷⁵.

Além disso, práticas de mercado vêm colocando em risco o direito à intimidade dos usuários brasileiros, pois os provedores, a quem pagamos para estarmos conectados, utilizam-se das informações advindas da navegação dos internautas para venderem esses dados para empresas especializadas em *marketing* direcionado. Assim, a informação privada do cidadão se torna um produto de altíssimo valor de mercado⁷⁶.

⁷¹ GREENWALD, 2014, p. 99.

⁷² *Ibidem*, p. 110.

⁷³ *Ibidem*, p. 127.

⁷⁴ *Ibidem*, p. 133-134.

⁷⁵ Disponível em: G1. **EUA grampearam Dilma, ex-ministros e avião presidencial, revela WikiLeaks.** Disponível em: <http://g1.globo.com/politica/noticia/2015/07/lista-revela-29-integrantes-do-governo-dilma-espionados-pelos-eua.html>. Acesso em: 17 dez. 2016.

⁷⁶ Nesse sentido: Aieta, 2014, p. 696.

Um destes exemplos foi vivenciado há poucos anos, quando foi noticiado que a *Serasa Experian*, definido como o “maior *bureau* de crédito do mundo fora dos Estados Unidos, detendo o mais extenso banco de dados da América Latina sobre consumidores, empresas e grupos econômicos”⁷⁷, teria firmado um acordo com o Tribunal Superior Eleitoral para ter acesso ao seu banco de dados, e, em troca, forneceria ao Judiciário Eleitoral mil certificados digitais – vez que figura como uma das entidades autorizadas pelo governo federal para emissão de tais certificados. Neste acordo, seria permitida a consulta, pelo banco de dados privado, do nome do eleitor, número e situação da inscrição eleitoral, além de eventuais óbitos e validação do nome da mãe e data de nascimento⁷⁸, visando uma utilização completamente desvirtuada daquela vivenciada quando da informação dos dados: a manutenção de situação eleitoral regular. Publicado no Diário Oficial da União em 23 de julho de 2013, tal acordo foi suspenso, em 08 de agosto do mesmo ano, de forma cautelar, ao argumento de que havia a possibilidade de quebra indevida de sigilo de dados dos eleitores⁷⁹. Apesar disso, existem indícios de que informações cadastrais de 141 milhões de eleitores foram disponibilizadas ao SERASA⁸⁰. Ainda que assim não fosse, remanesce pesadas dúvidas sobre a constitucionalidade e legitimidade deste tipo de convênio, pois as informações, repassadas com um fim específico, seriam utilizadas em malefício dos seus próprios detentores⁸¹.

Exemplo diverso é a parceria firmada entre o *Facebook* e o governo brasileiro, a fim de que seja ampliado o acesso à internet em território nacional. Segundo afirmou a ex-Presidente Dilma Rousseff, o acordo visa levar conexão de banda larga a populações de baixa renda e a áreas isoladas do país, entre as quais a Amazônia e

⁷⁷ SERASA EXPERIAN. Disponível em: <http://www.serasaexperian.com.br/quem-somos/institucional/>. Acesso em: 20 ago. /2023.

⁷⁸ Disponível em: <http://g1.globo.com/politica/noticia/2013/08/tse-firma-acordo-para-repassar-dados-d-e-eleitores-serasa.html>. Acesso em: 20 ago. 2023.

⁷⁹ Disponível em: <http://g1.globo.com/politica/noticia/2013/08/tse-decide-suspender-repasse-de-dados-de-eleitores-para-serasa.html>. Acesso em: 20 ago. 2023.

⁸⁰ Disponível em: http://istoe.com.br/318207_TSE+SUSPENDE+CONVENIO+QUE+REPASSOU+DA+DOS+DE+ELEITORES+A+SERASA/. Acesso em: 20 ago. 2023.

⁸¹ Importante esclarecer que não se trata aqui de mitigar o acesso às informações de caráter público, mas sim garantir ao cidadão que os dados fornecidos ao estado serão utilizados com um objetivo claro e específico. A bem da verdade, a única certeza possível neste ponto é que a existência de normativa especial quanto à proteção de dados pessoais permitiria um debate muito mais claro e seguro quanto a legitimidade e constitucionalidade deste tipo de acordo, que hoje ocorre (apesar de temporariamente suspenso) à margem da legalidade.

partes do Centro-Oeste⁸². Entretanto, considerando que o interesse de empresas como o *Facebook* é o de captar dados para fomento do *marketing* direcionado, certo é que a disposição da empresa norte-americana não busca a mera inclusão digital da população marginalizada, mas sim a ampliação de seu mercado, aproveitando-se de um país cuja teia normativa não tem se mostrado capaz de impedir a colheita indiscriminada de dados pessoais.

Por fim, imperioso mencionar o caso jurídico de maior repercussão em solo brasileiro dos últimos tempos: a denominada “Operação Lava Jato”. Referida operação – hoje contestada, em vários aspectos, no Supremo Tribunal Federal – foi responsável, após dois anos de sua deflagração, por contabilizar números como: 990 anos em penas acumuladas, 134 mandados de prisão expedidos e 93 condenações criminais⁸³.

A despeito das considerações que se possa fazer em relação ao mérito desta ação, chama a atenção, para os fins requeridos no presente trabalho, o volume de dados captados e armazenados durante as investigações promovidas no âmbito da operação: 1,2 milhão de *gigabytes*. Para tanto, foi desenvolvido um programa de computador denominado Indexador e Processador de Evidências Digitais (IPED), com a finalidade exclusiva de agilizar a análise dos dados coletados em computadores e servidores e principalmente após ações de busca e apreensão em operações da Polícia Federal⁸⁴.

Como garantir a integridade de tais dados, principalmente daqueles que se conectam a pessoas estranhas às apurações buscadas na demanda? Ainda mais importante: qual a responsabilidade dos órgãos estatais para com os dados pessoais coletados daqueles que não figuram como suspeitos de delitos, mas que mantiveram contato com as pessoas investigadas? Nunca existiu resposta concreta a tais

⁸² BBC News. **Dilma anuncia parceria com Facebook para ampliar acesso à internet**. Disponível em: http://www.bbc.com/portuguese/noticias/2015/04/150410_dilma_facebook_pai_jf. Acesso em: 20 ago. 2013.

⁸³G1. **Dois anos após primeira fase, Lava Jato soma penas de quase mil anos**. Disponível em: <http://g1.globo.com/pr/parana/noticia/2016/03/dois-anos-apos-primeira-fase-lava-jato-soma-penas-de-quase-mil-anos.html>. Acesso em: 20 ago. 2023.

⁸⁴Disponível em: <http://www1.folha.uol.com.br/poder/2017/01/1846272-neo-volume-de-dados-da-lava-jato-forca-pf-a-criar-novo-sistema.shtml>. Publicado em: 09 jan. 2017. Disponível em: Acesso em: 20 ago. 2023.

indagações. Os dados, ao que consta, restam armazenados, longe do alcance e controle de seus titulares.

O poder judiciário brasileiro também não tem sabido como lidar com o fluxo de dados e a realidade encontrada nos aplicativos de ambientes informatizados. Pouco tempo atrás, não raro nos deparamos com bloqueios de aplicativos de conversa, a exemplo do WhatsApp⁸⁵, por meio de ordens judiciais⁸⁶ que alcançavam não apenas os atores de determinada demanda judicial, mas sim toda a população. Tais situações denotavam, de um lado, falta de técnica dos membros da judicatura, e, de outro, o enfraquecimento de um poder local, emanado dos juízes, que não consegue lidar com potências globais, como o Facebook, atual dono do aplicativo WhatsApp, que atua sem se importar com fronteiras nem limites.

Ainda que há tempos não se vivenciem bloqueios ao *WhatsApp* como os frequentemente experimentados anos atrás, a questão não se mostra totalmente pacificada⁸⁷. Além disso, em tempo muito recente, o Supremo Tribunal Federal, órgão máximo do Poder Judiciário brasileiro, se utilizou do mesmo expediente – bloqueio de aplicativo de mensagens em razão de descumprimento de decisão judicial – para ver atendida uma requisição exarada por um de seus Ministros: no dia 18 de março de 2022, o Ministro Alexandre de Moraes, determinou que as plataformas digitais e provedores de internet tomassem medidas para impedir o uso do aplicativo de mensagens *Telegram* no país. Tal atitude se mostrou necessária, de acordo com o Ministro, em razão de a plataforma mostrar "total desprezo à Justiça brasileira", ao deixar de atender a comandos judiciais em várias ocasiões. Moraes lembrou que o

⁸⁵Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-deve-ser-bloqueado-decide-justica-do-rio.html>. Acesso em: 20 ago. 2023.

⁸⁶Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-bloqueado-relembre-todos-os-casos-de-suspensao-do-app.html>. Acesso em: 20 ago. 2023.

⁸⁷ Nesse contexto, pende de julgamento, pelo Supremo Tribunal Federal, a ADI proposta para questionar a constitucionalidade, principalmente, do art. 10, §2º, da Lei nº 12.965/2014, comumente conhecido como Marco Civil da Internet. Proposta pelo Partido Liberal (PL), a legenda pediu o reconhecimento da inconstitucionalidade da penalidade de suspensão temporária dos aplicativos de mensagens, devido à função social desse tipo de serviço. Referida demanda visa contestar, portanto, a possibilidade de suspensão de serviços de mensagem, como o *WhatsApp*, por descumprimento de ordens judiciais. Sobre a questão, consultar: CONSULTOR JURÍDICO. **STF vai julgar em sessão presencial se *WhatsApp* pode ser suspenso pela Justiça**. <https://www.conjur.com.br/2023-set-26/stf-julgar-whatsapp-suspensao-ordem-judicial>. Acesso em: 20 ago. 2023.

aplicativo operaria no território brasileiro sem indicação de representação legal, o que seria também incompatível com a “ordem constitucional vigente”⁸⁸.

Sobre o caso, de acordo com os documentos apresentados na demanda, a Polícia Federal teria empreendido esforços incansáveis para estabelecer contato com a plataforma *Telegram*, buscando transmitir ordens judiciais para bloquear perfis, solicitar informações de registro, obter a identificação de usuários e suspender a monetização de contas associadas a determinados usuários. Diante da ausência de resposta em todas as tentativas realizadas, as autoridades policiais optaram por recorrer à mais alta instância jurídica do País, a fim de obter uma decisão que impedisse o acesso. A decisão foi obtida; seu cumprimento, no entanto, se mostrou laborioso. Com efeito, repise-se, o Supremo Tribunal Federal, a mais alta Corte brasileira, guardiã precípua da Constituição, teve de determinar o bloqueio do aplicativo de mensagens, na medida em que não era nem respondida pela empresa atuante no Brasil, e que vive e lucra a partir dos dados pessoais que coleta dos nacionais e trata fora do país⁸⁹.

Após renovados silêncios, e vislumbrada a ordem de bloqueio, decidiu o CEO do *Telegram* pelo cumprimento da decisão: referida postura não foi acompanhada, todavia, de qualquer temor, reverencial ou não⁹⁰, de ter sobre si impostas sanções efetivas, capazes de desencorajar novos desrezos (e ilícitos), mas de um simples pedido de desculpas, justificando a ausência de resposta ao STF por um equívoco ao endereçar os e-mails de resposta⁹¹ – ainda que o caso fosse amplamente conhecido

⁸⁸ Sobre o assunto, ver: <https://canaltech.com.br/internet/bloqueio-do-telegram-no-brasil-e-determina-do-por-alexandre-de-moraes-do-stf-211921/>. Acesso em: 20 ago. 2023

⁸⁹ A íntegra da decisão pode ser consultada em: CONJUR. **Petição 9.935**, Distrito Federal. <https://www.conjur.com.br/dl/alexandre-moraes-ordena-bloqueio.pdf>. Acesso em: 20 ago. 2023.

⁹⁰ Tanto é que, no ano de 2023, o Ministro Alexandre de Moraes teve de, novamente, lançar mão desse expediente altamente questionável, concedendo prazo de uma hora para que o aplicativo Telegram excluísse mensagens enviadas aos seus usuários a respeito do Projeto de Lei (PL) 2630, conhecido como PL das *Fake News*, que trata da regulação dos provedores de redes sociais e de serviços de mensagem privada, sob pena de suspensão das atividades do aplicativo em todo país. A íntegra da decisão pode ser consultada em: <https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/Decisa771oTelegramAssinada1.pdf>. Acesso em: 20 ago. 2023.

⁹¹ Sobre o assunto, ver: CANAL TECH. **Após bloqueio no Brasil, CEO do Telegram pede desculpas ao STF por negligência**. Disponível em: <https://canaltech.com.br/juridico/apos-bloqueio-no-brasil-ceo-do-telegram-pede-desculpas-ao-stf-por-negligencia-211942/>. Acesso em: 20 ago. 2023.

da sociedade brasileira, e estivesse, diariamente, nos mais importantes jornais brasileiros⁹². Cumprida a decisão, a ordem de bloqueio foi revogada⁹³.

Haveria, em verdade, uma miríade de exemplos de como o Brasil e os brasileiros têm sido alvo, nos últimos anos, de vazamentos indiscriminados de dados pessoais, capturados com os mais diferentes objetivos, mas que convergem, sempre, para o mais escuso deles: ao final, sempre o tratamento não consentido, para fins que se tornam, por eles mesmos, ou em razão do não consentimento, ilegais. Desde 2011, ano em o serviço *Play Station Network*, mantido pela empresa Sony, foi invadido e os dados de 77 milhões de usuários foram vazados⁹⁴, dos quais muitos brasileiros – em número nunca totalmente precisados – foram vítimas, passando pelo ano de 2021, em que dois “megavazamentos” de dados ocorreram: um, de 223 milhões de brasileiros – número maior do que a população do país, estimada em 212 milhões de habitantes à época, porque incluía dados de pessoas falecidas – cujas informações expostas variavam desde nome, sexo, data de nascimento e CPF, até tabelas com dados de veículos e listas com CNPJs⁹⁵, em caso nunca totalmente explicado⁹⁶ – e outro, de cerca de 3,2 bilhões de senhas de e-mails do mundo inteiro, dos quais 10 milhões eram de e-mails de titulares brasileiros, e por volta de 70 mil usuários eram do setor público nacional (o domínio mais exposto foi o "caixa.gov.br" com cerca de 2.197 senhas vazadas), descoberto em fóruns da *deep web*⁹⁷, e chegando aos tempos mais recentes, em que quase 1 bilhão de dados pessoais foram vazados, no Brasil, no ano de 2022 – situação em que os criminosos, com vistas à comercialização de

⁹² Apenas para citar, como exemplo, outro portal que veiculou, à época, notícias sobre o ocorrido: <https://www.bbc.com/portuguese/brasil-60801662>. Acesso em: 20 ago. 2023.

⁹³ A íntegra da decisão pode ser consultada em: <https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/ano/DecisaoTelegram20mar.pdf>. Acesso em: 20 ago. 2023.

⁹⁴ Sobre o assunto, ver: JUSBRASIL. **Os efeitos do vazamento de dados das Redes da Sony na legislação brasileira**. <https://www.jusbrasil.com.br/noticias/os-efeitos-do-vazamento-de-dados-das-redes-da-sony-na-legislacao-brasileira/2664002>. Também: https://www.bbc.com/portuguese/noticias/2011/04/110427_sony_hacker_bg. Acesso em: 21 ago. 2023.

⁹⁵ Sobre o assunto, ver: G1. **Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber**. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml>. Acesso em: 21 ago. 2023.

⁹⁶ Sobre o assunto, ver: TECNOBLOG. **Megavazamento de 223 milhões de CPFs: um ano se passou e ainda há perguntas sem resposta**. <https://tecnoblog.net/especiais/megavazamento-de-223-milhoes-de-cpfs-um-ano-se-passou-e-ainda-ha-perguntas-sem-resposta/>. Acesso em: 21 ago. 2023.

⁹⁷ Sobre o assunto, ver: PODER 360. **Megavazamento global expõe 10 milhões de senhas de e-mails brasileiros**. Disponível em: <https://www.poder360.com.br/tecnologia/megavazamento-global-expoe-10-milhoes-de-senhas-de-e-mails-brasileiros/>. Acesso em: 21 ago. 2023.

tais dados, têm acesso até a dados do sistema CórteX, do Ministério da Justiça⁹⁸ – o que se vê é o crescimento exponencial dessa atividade, que chega ao ano de 2023 como um assunto acerca do qual não se pode mais tergiversar, acreditando que a legislação protetiva de dados pessoais tem cumprido o papel a que deve, realmente, se destinar: tutelar os cidadãos brasileiros dos ataques ao seu direito fundamental de proteção ao bem mais precioso que, hoje, ostentam para o capital mundial – seus dados pessoais.

Em vistas do que se percebe nos últimos anos, não surpreende que, no presente ano de 2023, já se tenham notícias de vazamentos de quase 6 milhões de dados de saúde de brasileiras e brasileiros⁹⁹; de vazamentos de dados de nacionais por meio do aplicativo de Inteligência Artificial “*ChatGPT*” – figurando, o país, em terceiro lugar entre os mais atingidos por essa exposição¹⁰⁰ – e que, todos os meses, cerca de 10 milhões de brasileiros tenham dados, como logins e senhas, expostos ilegalmente no ambiente virtual¹⁰¹: o número mostra um crescimento vertiginoso, de mais de 60%, em relação ao que foi registrado no ano passado, quando a média era de, aproximadamente, 6 milhões de exposições de credenciais por mês – ano em que o país foi considerado como o de maior número de credenciais vazadas por criminosos¹⁰². Todos esses indicativos nos colocam em uma posição preocupante; tanto é que estudo conduzido pela empresa norte-americana de cibersegurança *Tenable*¹⁰³ indicou que, de todos os dados vazados no mundo no ano de 2022, cerca de 112 *terabytes* de dados – ou seja, quase metade dos dados vazados no mundo

⁹⁸ Sobre o assunto, ver: <https://oglobo.globo.com/economia/defesa-do-consumidor/noticia/2023/06/do-ssies-com-dados-publicos-e-privados-municipiam-golpes-eletronicos.ghtml>. Acesso em: 21 ago. 2023.

⁹⁹ Sobre o assunto, ver: CANAL TECH. **Vazamento expõe quase 6 milhões de dados de saúde dos brasileiros**. Disponível em: <https://canaltech.com.br/seguranca/vazamento-expoe-quase-6-milhoes-de-dados-de-saude-dos-brasileiros-246314/>. Acesso em: 21 ago. 2023.

¹⁰⁰ Sobre o assunto, ver: TECNOBLOG. **Megavazamento de 223 milhões de CPFs: um ano se passou e ainda há perguntas sem resposta**. Disponível em: <https://tecnoblog.net/especiais/megavazamento-de-223-milhoes-de-cpfs-um-ano-se-passou-e-ainda-ha-perguntas-sem-resposta/>. Acesso em: 21 ago. 2023.

¹⁰¹ Os números são da empresa de segurança *Apura Cyber Intelligence*, Sobre o assunto, ver: CANAL TECH. **10 milhões de brasileiros têm dados vazados todos os meses**. Disponível em: <https://canaltech.com.br/seguranca/10-milhoes-de-brasileiros-tem-dados-vazados-todos-os-meses-254304/>. Acesso em: 21 ago. 2023.

¹⁰² Sobre o assunto, ver: CANAL TECH. **Brasil foi o país com mais credenciais vazadas em 2022**. Disponível em: <https://canaltech.com.br/seguranca/brasil-foi-o-pais-com-mais-credenciais-vazadas-em-2022-249474/>. Acesso em: 21 ago. 2023.

¹⁰³ Para consulta à pesquisa, ver: TENABLE. **Relatório do cenário de ameaças de 2022 da Tenable**. Disponível em: <https://pt-br.tenable.com/cyber-exposure/tenable-2022-threat-landscape-report>. Acesso em: 21 ago. 2023.

inteiro (mais precisamente, 43% de um total de 257 *terabytes*) – foram vazados somente no Brasil¹⁰⁴.

A tais vazamentos ilegais de dados devem ser somadas duas outras questões igualmente relevantes para a proteção de dados no Brasil: a primeira, correspondente ao próprio interesse governamental na captura e tratamento ilegal de dados, com viés escuso e contra seu próprio povo; e a segunda, referente à captura e tratamento diuturno de dados pelo viés considerado “lícito”, ou seja, pela atividade precípua das gigantes companhias tecnológicas, que se alimentam, financeiramente, dessa atuação. O segundo assunto, principalmente, será melhor detalhado e abordado no capítulo subsequente.

Quanto ao papel do governo brasileiro na captura e tratamento de dados pessoais, figuraria o Brasil como exceção dentre vários países tecnologicamente incluídos na globalização, inexistindo em solo pátrio programa de espionagem, mediante captura de dados pessoais, a exemplo do vislumbrado nos Estados Unidos¹⁰⁵? Órgãos como a Agência Brasileira de Inteligência negligenciam o imenso potencial de controle advindo da colheita de dados pessoais? Ou a fazem, a exemplo de outros países, à margem da Lei¹⁰⁶?

Pelo que podemos verificar, algum indicativo de resposta foi dado muito recentemente: no dia 14 de março de 2023, documentos obtidos pelo “O GLOBO” e relatos de servidores revelaram, em reportagem assinada por Dimitrius Dantas, Patrik Camporez e Thiago Bronzatto, que a Agência Brasileira de Inteligência (Abin), nos primeiros três anos do governo Jair Bolsonaro (2018-2021), operou um sistema secreto de monitoramento de cidadãos em todo o Brasil. Por meio do software denominado “*FirstMile*” – que custou aos cofres nacionais, mediante dispensa de licitação e ainda na gestão do então Presidente Michel Temer, no fim do ano de 2018,

¹⁰⁴ Sobre o assunto, ver: Disponível em: NIC.BR. **Quase metade dos dados vazados no mundo são brasileiros, indica estudo**. <https://www.nic.br/noticia/na-midia/quase-metade-dos-dados-vazados-no-mundo-sao-brasileiros-indica-estudo/>. Acesso em: 21 ago. 2023.

¹⁰⁵ A descrição do programa de espionagem revelado por Edward Snowden será, igualmente, melhor detalhada no capítulo seguinte.

¹⁰⁶ Nesse sentido o alerta de Stefano Rodotà: “Às novas formas de coleta e tratamento de informações, possibilitadas sobretudo pelo recurso a computadores, adicione-se a crescente necessidade de dados por parte das instituições públicas e privadas; como não é imaginável uma ação que vá de encontro a esta tendência, comum a todas as organizações sociais modernas, é necessário considerar de forma realista tal situação, analisando as transformações que causa na distribuição e no uso do poder pelas estruturas públicas e privadas” (RODOTÁ, 2008, p. 24).

R\$ 5,7 milhões – a Abin tinha a capacidade de rastrear a localização de até 10 mil proprietários de celulares a cada 12 meses, sem seguir protocolos oficiais. O programa foi desenvolvido pela empresa israelense *Cognyte* e permitia acessar o histórico de deslocamentos, além de criar alertas em tempo real. A questão gerou investigações internas, questionamentos sobre a legalidade e a possível violação do direito à privacidade, enquanto a Abin alegava operar em um "limbo legal", e se recusava a comentar o caso em razão de "sigilo contratual"¹⁰⁷.

O uso da ferramenta chegou a ser mencionado em uma decisão judicial relacionada a uma operação da Polícia Federal que investigava suspeitas de vazamentos de informações por representantes comerciais do programa no Brasil. Tal fato propiciou, tempos depois, em 20 de outubro de 2023, em ação autorizada pelo ministro do Supremo Tribunal Federal, Alexandre de Moraes – que determinou, entre outros, o cumprimento de 25 mandados de busca e apreensão e dois de prisão preventiva nos estados de São Paulo, Santa Catarina, Paraná e Goiás e no Distrito Federal, além do afastamento do cargo de diretores atuais da Abin e a prisão de dois servidores da Agência – o desenrolar de uma apuração que busca confirmar o uso de sistemas de GPS para rastrear celulares sem autorização judicial. Para tanto, a rede de telefonia brasileira teria sido invadida diversas vezes, com a utilização do serviço adquirido com recursos públicos – o software denominado "*FirstMile*"¹⁰⁸. Ainda, segundo a investigação da Polícia Federal, a tecnologia de empresa israelense teria sido usada para monitorar irregularmente a localização de celulares de servidores públicos, políticos, policiais, advogados, jornalistas e até mesmo de juízes¹⁰⁹.

Ainda nesse contexto, conforme informações da *Data Privacy Brasil*, o sistema não apenas identificava a localização aproximada dos dispositivos, mas também tinha a capacidade de gerar alertas com base na rotina de movimentação dos alvos de interesse. Em maio de 2019, a Associação Catarinense de Empresas de Tecnologia (Acate) identificou a empresa *Suntech* como a representante e suposta desenvolvedora do software "*VERINT First Mile – Geolocalização Celular Remota*" no

¹⁰⁷Disponível em: <https://oglobo.globo.com/politica/noticia/2023/03/abin-de-bolsonaro-usou-programa-secreto-para-monitorar-localizacao-de-pessoas-por-meio-do-celular.ghtml>. Acesso em: 20 out. 2023.

¹⁰⁸Disponível em: <https://g1.globo.com/politica/noticia/2023/10/20/policia-federal-abin-geoloc-alizacao.ghtml>. Acesso em: 20 out. 2023.

¹⁰⁹Disponível em: <https://g1.globo.com/tecnologia/noticia/2023/10/20/fist-mile-o-que-se-sabe-sobre-o-software-espiao-usado-pela-abin.ghtml>. Acesso em: 20 out. 2023.

Brasil, embora não tenha sido confirmado se a Abin adquiriu o programa por meio dessa empresa¹¹⁰. Por fim, uma reportagem da Forbes, datada de dezembro de 2020, denunciou a atuação de empresas israelenses que coletavam dados de localização de pessoas em diversos países, incluindo a *Cognyte/Verint*, que comercializava uma variedade de ferramentas de espionagem. Entre as tecnologias vendidas, uma delas permitia rastrear a localização de indivíduos com base em seus números de telefone, usando torres de celular próximas¹¹¹.

Referido caso demonstra, com pujança, como o Brasil – no caso, as brasileiras e os brasileiros – além de sofrer diariamente com o vazamento de dados pessoais por meio de atividades privadas manifestamente ilícitas, também se vê atacado por programas governamentais sub-reptícios de captura e tratamento de dados, a partir do que se indaga: qual o interesse do Estado em proteger os dados pessoais, sendo que figura como um dos maiores interessados em seu conteúdo?

Não há necessidade, inclusive, que o Estado, para violar o direito de proteção aos dados pessoais, atue nas sombras. No ano de 2020, necessário se fez o ajuizamento de Ação Direta de Inconstitucionalidade voltada a questionar a legitimidade de órgãos e de entidades da administração pública federal compartilharem dados pessoais entre si. Por meio da ADI 6389, em que se defendeu a inconstitucionalidade do art. 2º, caput e §§ 1º e 3º da MP 954/2020 – medida provisória que obrigava a disponibilização de dados pessoais dos usuários de operadoras de telefonia fixa e móvel com o instituto brasileiro de Geografia e estatística (IBGE) – o jurista brasileiro de elevada importância e saudosa memória, Professor Danilo Doneda, argumentou, com brilhantismo, que o caso dizia respeito não somente a pesquisas realizadas pelo IBGE, mas “sobre os próprios parâmetros constitucionais da proteção de dados no Brasil e, ao final, ao valor e significado dos dados pessoais dos brasileiros para a nossa liberdade, personalidade e democracia”¹¹². Em razão de referida ADI, o STF suspendeu o compartilhamento de

¹¹⁰Disponível em: <https://www.acate.com.br/wp-content/uploads/2019/05/Atestado-de-Exclusividade-SUNTECH-16.05.19.docx-1-1.pdf>. Acesso em: 20 out. 2023.

¹¹¹ Disponível em: <https://www.forbes.com/sites/thomasbrewster/2020/12/11/exclusive-israeli-surveillance-companies-are-siphoning-masses-of-location-data-from-smartphone-apps/?sh=5fd5c1e138fc>. Acesso em: 20 out. 2023.

¹¹² A íntegra da sustentação oral realizada pelo Professor Danilo Doneda pode ser conferida em: <https://civilistica.emnuvens.com.br/redc/article/view/519>. Acesso em: 21 ago. 2023.

dados de usuários de telefônicas com IBGE; para a maioria dos ministros, a previsão contida na Medida Provisória nº 954/2020 violava o direito constitucional ao sigilo de dados, entre outros¹¹³.

As intensas agressões aos dados pessoais de brasileiros e brasileiras não suplantam, no entanto, o panorama que se instala a partir de uma pretensa normalidade. O tratamento e captura de dados pessoais funciona como a engrenagem mais poderosa do capitalismo em seu estágio mais contemporâneo – realidade em que a matéria-prima é a captura com ares de legalidade e condescendência. Nesse contexto, as maiores ameaças vêm, efetivamente, de fora do país. É o que nos mostrará a abordagem do capítulo seguinte, voltada a desnudar, entendido o poder da privacidade, o fenômeno denominado “colonialismo de dados”, em razão do qual, e contra o qual, principalmente, se verifica que a legislação brasileira, conforme posta, é inócua aos fins que se destina.

Compreender todo esse complexo panorama, e não apenas compreendê-lo, mas efetivamente utilizá-lo para compor uma normatividade capaz de tutelar os interesses do povo brasileiro e o efetivo cultivo de uma Democracia verdadeira, é o que se denomina de tropicalização do pensamento sobre proteção de dados pessoais. Significa, portanto, compreender a posição do Brasil no mundo econômico-globalizado, em que nossa condição de país periférico nos lança, acaso nos submetamos ao “jogo” dos poderes mundiais, hodiernamente representados pelas práticas e ideais do neoliberalismo, na imensa maioria das vezes, à posição de caça para o caçador, de presa para o predador, cujo banquete é servido às custas, sempre, dos mais vulneráveis, em um contexto em que a legislação doméstica serve mais como um mecanismo de dominação, garantindo o trânsito dos dados das brasileiras e brasileiros com o estrangeiro, do que como proteção aos habitantes de nossa terra.

Tropicalizar o pensamento sobre a proteção de dados pessoais significa, ao fim e ao cabo, realizar, *mutatis mutandis*, aquilo que Guerreiro Ramos trata enquanto aspectos da redução sociológica. O autor destaca três elementos essenciais relacionados à redução sociológica: primeiro, ela busca identificar as condições ontológicas e existenciais da cultura brasileira; segundo, enfatiza a necessidade de

¹¹³ Disponível em: <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902&ori=1>. Acesso em: 21 ago. 2023.

compreender as condições críticas para o desenvolvimento da ciência nacional; e terceiro, coloca a cultura brasileira como objeto primordial da sociologia no Brasil. Em essência, o autor argumenta que a sociologia no Brasil deve ser sensível às características e desafios únicos do país, evitando uma abordagem meramente institucionalizada que não leve em consideração as especificidades culturais e os problemas concretos do Brasil (RAMOS, 2016).

O pensamento sobre o direito à proteção de dados pessoais no Brasil carece, portanto, de uma imprescindível e correspondente redução sociológica. Consoante afirmado na introdução do presente capítulo, importantes escritos sobre o tema, de juristas do mais alto quilate, deixam, por vezes e muitas vezes, tal aspecto relegado a um plano diferente do primeiro.

Não se pode negar, nessas circunstâncias, que boa parte da população brasileira é, atualmente, altamente dependente da tecnologia. Os estudos mostram que a internet é, atualmente, acessível em 90% dos domicílios brasileiros, e que a grande maioria dos nacionais detêm, por exemplo, um celular¹¹⁴. Tal realidade de consumo, no entanto, não é simétrica em todo o território nacional; o Brasil goza, com efeito, de disparidades atroz, nos colocando, frequentemente, como um dos países mais desiguais do mundo¹¹⁵.

Além disso, a própria consciência acerca dos riscos advindos da captura e tratamento de dados pessoais são profundamente incipientes. Ainda que a

¹¹⁴ De acordo com a Pesquisa Nacional por Amostra de Domicílios Contínua – PNAD Contínua sobre o módulo de Tecnologia da Informação e Comunicação – TIC, realizada pelo IBGE, em 2021, 155,2 milhões de pessoas de 10 anos ou mais de idade tinham telefone móvel celular para uso pessoal, o que correspondia a 84,4% da população dessa faixa etária, percentual maior que o estimado para 2019 (81,4%). Contudo, havia grande discrepância entre os percentuais conforme a situação do domicílio. Enquanto 87,1% das pessoas que viviam em área urbana tinham telefone móvel celular para uso pessoal, esse percentual era de 67,6% entre as pessoas da área rural. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101963_informativo.pdf. Acesso em: 22 ago. 2023.

¹¹⁵ Um relatório sobre a riqueza global em 2021, realizado pelo banco Credit Suisse, aponta que o Brasil, a partir do Índice de Gini, continua sendo um dos países mais desiguais do mundo, superado por apenas meia dúzia em uma lista de 127 países. Segundo a pesquisa, no ano 2000, o grupo dos brasileiros mais ricos (2,1 milhões de pessoas ou 1% da população) detinha 44,2% de toda a renda do país; em 2020, referida parcela da população era dona de quase metade da riqueza nacional, ou seja, 49,6%: o que significa que os ricos ficaram ainda mais ricos em 5,4% nas últimas duas décadas. Disponível em: <https://www.credit-suisse.com/about-us/en/reports-research/global-wealth-report.html>. Acesso em: 22 ago. 2023. O Relatório de Desenvolvimento Humano (RDH) elaborado pela Organização das Nações Unidas (ONU), por sua vez, responsável por analisar essa concentração de riquezas, coloca o Brasil em segundo lugar no *ranking* de má distribuição de renda entre a população – atrás, apenas, do Catar. Disponível em: <https://pe.unit.br/blog/noticias/pandemia-agravou-o-aumento-da-pobreza-no-brasil/>. Acesso em: 22 ago. 2023.

Constituição da República Federativa do Brasil preveja, em seu art. 205, *caput*, como objetivo do ensino nacional, a educação para a cidadania, e por mais que o direito à proteção dos dados pessoais constitua, atualmente, um direito fundamental, e que se considere sua fulcral importância para a manutenção e desenvolvimento de uma democracia saudável, o assunto está longe de povoar a mente dos jovens educandos (e quem dirá, portanto, da população adulta e há tempo egressa do sistema escolar). A reforma do ensino médio, nesse contexto, tem sido alvo de constantes ataques, mormente em razão de sua vinculação e formatação a interesses estrangeiros e do mercado¹¹⁶ – interesses que também convergem para a captura e tratamento indiscriminado de dados pessoais.

Sem dúvida que estudos absolutamente técnicos sobre intrincadas questões jurídicas envolvendo aspectos técnicos designáveis por estrangeirismos, visando tutelar interesses, em sua maioria, mercadológicos, têm e terão sempre espaço na literatura jurídica nacional. E para tais, quiçá, a aclimação de pensamento seja, em alguma medida, dispensável.

Diversa, no entanto, deve ser a literatura jurídica que queira se debruçar sobre os elementos mais fulcrais do ordenamento jurídico brasileiro, em uma genuína preocupação, *v.g.*, com o Estado Democrático de Direito, e, em razão disso, com os direitos e garantias fundamentais – entre eles, o direito de proteção aos dados pessoais. Razão pela qual, desejando-se a inserção nesse segundo grupo, é que se passa a analisar aspectos que, ao final, buscarão desnudar questões que auxiliem, justamente, em uma redução sociológica capaz de conduzir a uma tropicalização do pensamento brasileiro sobre a proteção dos dados pessoais, no que toca, especificamente, ao dever, e não faculdade, de se emitirem, pela ANPD, para a legítima transferência internacional de dados pessoais, “decisões de adequação”.

¹¹⁶ Sobre a questão: Zanatta (2019).

2.4 As tradições jurídicas, a “decisão de adequação” e o Brasil: entre traduções e “traições”

O tema referente às “tradições” jurídicas permeia, de há muito, o ambiente forense e acadêmico¹¹⁷. Por questões de reforço argumentativo, ou mesmo de conforto intelectual, não raro, juristas promovem o agrupamento de ideias, conceitos e teorias em determinadas “escolas” ou “correntes”, supostamente elaboradas, conscientemente, em determinado período histórico e em locais geograficamente determinados¹¹⁸.

Essas tentativas de agrupar em nichos específicos determinadas formas jurídicas de pensar histórica e/ou geograficamente localizadas permitem juristas, e também historiadores do direito, exercitar uma tarefa com potencial científico, mas também, caso não filtrada pela metodologia escoreta¹¹⁹, muito própria da simples forma humana de pensar¹²⁰: a comparação. Isso porque, identificadas as características gerais das tais “escolas” ou “correntes”, torna-se por vezes irresistível, de maneira subsequente, compará-las, a fim de se verificar se aqui ou acolá, se ontem e hoje, se em tempos mais ou menos remotos, pensavam as sociedades o direito de

¹¹⁷ Nesse sentido, romanistas e historiadores do direito se ocupam da denominada “recepção” do direito romano pelos períodos históricos posteriores, seja na Idade Média, seja na primeira modernidade. Nesse sentido: Fonseca, 2020, p. 4.

¹¹⁸ *Ibidem*, p. 1.

¹¹⁹ A complexa atividade científica derivada da História do Direito é descrita por Michael Stolleis, em capítulo dedicado à metodologia: *cada geração encontra as suas fontes e lê os textos há muito conhecidos de uma nova maneira, colocando diferentes ênfases na história das pessoas, na história dos acontecimentos ou na história das estruturas. Não há um caminho seguro no passado, que seria pavimentado com ‘fatos objetivos’ inquestionáveis. O passado como construção é sempre recriado, ao mesmo tempo que as notícias de todas as formas são lidas, interpretadas e unificadas nas imagens mais coerentes possíveis. Determinar como foi ‘realmente’ ou ‘de verdade’ é impossível, porque os próprios processos, no momento da sua formação, são percebidos de maneira multiperspectiva e tradicional. Disponível está, portanto, apenas a interpretação mais imparcial possível, apoiada pelas fontes, pela crítica das fontes e também dirigida pela autocrítica, que seja aceita pela maioria da comunidade científica”. (STOLLEIS, 2020, p. 60-61).*

¹²⁰ Nesse sentido, a lição tomada de Richard H. Thaler e Cass R. Sunstein, ao reproduzirem os estudos dos psicólogos israelenses Amos Tversky e Daniel Kahneman, responsáveis por identificar três heurísticas, e correspondentes vieses, na forma humana de pensar: ancoragem, disponibilidade e representatividade. Essa última – representatividade – também é definida como “heurística da similaridade”, ao reconhecer a constante ligação das opiniões humanas à atividade comparativa. Conforme os autores: “a ideia é que, quando perguntamos qual a probabilidade de que A pertença à categoria B, as pessoas (sobretudo seus Sistemas Automáticos) respondem com base na semelhança que enxergam entre A e a imagem ou estereótipo de B (ou seja, se A é ‘representativo’ de B). Assim como as outras duas heurísticas, esta é usada porque em geral funciona. [...] Os vieses costumam surgir quando há divergência entre similaridade e frequência. [...] Muitas vezes enxergamos padrões porque, ao observar as evidências, construímos nossos próprios testes informais” (THALER; SUNSTEIN, 2019, p. 37-39).

maneira similar, se o viviam com grande diferença, ou, ainda, se o produziam científica e intelectualmente com convergências ou divergências.

Não se trata aqui de rebaixar a perspectiva comparada do estudo do direito. Mas sim de reconhecer que seu exercício demanda uma inafastável responsabilidade hermenêutica, em razão da não rara problemática que envolve suas premissas: a utilização das tais “escolas” e “correntes” como axiomas para comparação. Na avidez de se apresentar, com verniz intelectual e acadêmico, conceitos jurídicos de maneira clara e erudita, com a pretensa capacidade de simplificar, em conceitos facilmente apreensíveis, fenômenos complexos, acabam juristas e historiadores por encaixar em determinadas “culturas jurídicas” ideias dissonantes, continuidades artificiais e formas desiguais de pensar e viver o direito. Exemplo do que se afirma é a dicotomia elaborada por certos autores entre os ditos “locais de produção” e “locais de recepção”: os primeiros, responsáveis por gestar, com absoluta genialidade e originalidade, conceitos e sistemas de direito, e os segundos, de absorver e adaptar tais conceitos e sistemas, em verdadeiras tentativas de transplante das criações realizadas, por exemplo, na Europa e nos Estados Unidos (polos de produção) para a realidade jurídica Latino-americana (polo de recepção)¹²¹.

Ocorre que, consoante sobredito, nem a realidade europeia, *v.g.*, goza da linearidade e homogeneidade anunciadas nas “escolas” e “correntes” jurídicas –ainda que similitudes e contornos importantes tenham existindo, como nas denominadas tradições francesa e germânica, cujas ideias não se espalhavam, no entanto, de maneira padronizada, nas realidades portuguesa, espanhola e italiana – nem a Latino-americana – em razão de sua multiculturalidade, produto de diferentes colonizações, como a espanhola, a francesa e a portuguesa, entre outras – conta com experiências jurídicas uniformes. Por esse motivo, compreender que vivências tão diversas tenham se prestado, uma ao papel de polo produtor de teorias e sistemas de direito, com absoluta coerência, e a outra, ao de simples mimese dessas realidades, não condiz com uma compreensão histórica comprometida com a complexidade desses locais e períodos históricos¹²².

¹²¹ Referida terminologia é emprestada, por Ricardo Marcelo Fonseca, dos estudos de Diego Lopez Medina. Nesse sentido, FONSECA, 2020, p. 2.

¹²² *Ibidem*, p. 4.

Daí decorre, portanto, o problema de se utilizar, de maneira estanque, o conceito de “tradição” jurídica. Há, sem dúvida, influências europeias e norte-americanas naquilo que se produziu ao sul do mundo: o fenômeno codificador, a separação de poderes, o Constitucionalismo, entre outros. Mas, muito mais do que o simples transplante jurídico, o que se operaram entre as diferentes realidades, entre os diversos locais, não de produção e de recepção de conceitos e teorias, mas de vivências sociais reguladas pelo direito, passíveis, portanto, de intercâmbios e influências nos pensamentos da juridicidade, foram diferentes maneiras de adaptação e entendimento de legislações e práticas jurídicas estrangeiras, ainda que essas, porventura, tenham sido impostas aos locais dominados. A internalização de questões jurídicas advindas de realidades diferentes, de maneira imperativa ou por simples influência, passam, obrigatoriamente, por uma releitura de seu entendimento e de suas possibilidades no local em que passa a ser praticada. E é justamente por conta dessa forçosa releitura, não raro realizada, inclusive, textualmente, com a necessidade de se transmutar, de uma língua para outra, o ordenamento jurídico, é que avulta a importância da tradução, e de sua teoria subjacente, para compreensão dessas questões.

Compreender historicamente o passado, mais do que tornear ideias para encaixá-las em tradições pré-formatadas, envolve traduzir questões de tempos e lugares diversos para a atualidade. Nos dizeres de Ricardo Marcelo Fonseca, “é apropriar-se do que ocorreu no passado para, num procedimento complexo, buscar dar um sentido num tempo diferente”¹²³. O conceito de tradução, portanto, tem o condão de prestar grande auxílio na tarefa de se evitar as esparrelas decorrentes do estudo dos “transplantes” jurídicos enquanto mera tradição, cuja mofada dicotomia insiste em apresentar polos simplesmente produtores e outros meramente receptores de tais tradições.

E isso ocorre justamente porque o historiador, e mesmo o comparatista, ao tomar consciência de seu papel como tradutor, passa a se preocupar não apenas com o que seria um simples transplante de ideias e conceitos entre tempos e lugares, mas com a descontextualização e recontextualização que sofrem as culturas jurídicas e os conceitos ditos transplantados. Compreender a importância da linguagem e da

¹²³ *Ibidem*, p. 6.

narrativa na construção da realidade, com sua metodologia correspondente¹²⁴, indica o quão importante se apresenta a tarefa de interpretação do que exprimiram as diferentes culturas jurídicas, para, a partir de então, se compreender os contornos assumidos pelo diálogo entre elas¹²⁵.

É importante ressaltar, nesse ponto, que a história do direito cuida, por meio da linguagem, de *dar na atualidade sentido ao que ocorreu no passado*. Ao se extrair, do interior dessa ciência, as premissas metodológicas para se trabalhar com questões de caráter bastante atual – as legislações protetivas de dados pessoais – deve-se explicitar em que bases isso se dá, de maneira a situar a compreensão (e eventuais críticas) do leitor/investigador. Acredita-se, nesse contexto, que os objetos de estudo, quais sejam, o Regulamento Geral de Proteção de Dados europeu e a Lei Geral de Proteção de Dados brasileira apresentam-se como normativas promulgadas, vigentes, cada qual, em seus locais de aplicação. Nada impede, diante disso, que se promova, assim como realizado por autores consagrados¹²⁶, que também analisam questões atinentes ao tempo presente, um recorte metodológico¹²⁷: considera-se o momento histórico em que gestados tais textos normativos como findo, com o único objetivo de situar-se, na condição de observador, em local externo ao do objeto, focando-se nele como elemento separado do sujeito. Essa artificialidade, conforme

¹²⁴ STOLLEIS, 2020, p. 33.

¹²⁵ Ricardo Marcelo Fonseca, ao explicitar os ensinamentos de Peter Burke (BURKE e HSIA, 2009) acerca dos “regimes de tradução” e sua importância para a história cultural, aponta, a partir do teórico inglês, que os procedimentos de pesquisa nessa seara devem buscar responder a seis grandes perguntas: Quem traduz? Com que intenção se traduz? O que se traduz? Para quem? De que maneira? Com que consequências? Na forma apresentada por Fonseca: “verificar o modo sempre peculiar e contextualizado como um tempo passado se apropria de outra tradição cultural, tentando entender os mecanismos e os interesses envolvidos nessa apropriação, é algo que tem um grande potencial de dizer algo sobre o nosso passado”. (FONSECA, 2020, p. 7).

¹²⁶ Assim se comporta, por exemplo, Zygmunt Bauman, ao apresentar sua teoria acerca da atual modernidade, ou, conforme prefere denominar, *modernidade líquida*. A questão central colocada pelo sociólogo polonês para estabelecer uma era “pós-moderna” repousa sobre a possibilidade de abordagem da “modernidade” sob uma perspectiva externa, focada como objeto separado do sujeito, permitindo assim que esse se posicione em outro nível de observação – a atual modernidade, ou pós-modernidade. Nesse sentido aduz que: “à diferença da noção de uma sociedade pós-industrial, o conceito de pós-modernidade refere-se a uma qualidade diferente do clima intelectual, a uma postura distintamente metacultural, a uma autoconsciência diversa de sua era. Um dos elementos básicos, senão o elemento básico, dessa autoconsciência é a compreensão de que a modernidade acabou, de que ela é um capítulo fechado na história, que pode agora ser contemplado em sua inteireza, com conhecimento retrospectivo de suas realizações práticas, bem como de suas esperanças teóricas” (BAUMAN, 2001, p. 166).

¹²⁷ Acerca da artificialidade do recorte realizado pelo autor, de natureza metodológica, Bauman esclarece ainda que “a sociedade que entra no século XXI não é menos moderna que a que entrou no século XX; o máximo que se pode dizer é que ela é moderna de um modo diferente”. *Ibidem*, p. 36.

sobredito, constitui vantagem metodológica que, uma vez manifestada consciente e transparente no trabalho, permite ao leitor/investigador o efetivo conhecimento daquilo que se apresenta e da forma como se apresenta, sem traí-lo. Daí é que se extrai a licitude da tarefa.

No entanto, ainda que viável metodologicamente, entender as condições em que se promoveram, no passado, traduções jurídicas, e traduzi-las para o presente, significa não apenas conjugar elementos linguísticos, com necessário apoio nas teorias da tradução, mas visitas prementes ao contexto em que realizadas ditas traduções, identificando, consoante sobredito, descontextualizações e recontextualizações que impactaram e formataram as respectivas culturas jurídicas. Nesse diálogo entre línguas e tempos, de transposição de realidades diversas e complexas, pressupor-se negociação, manipulação e adaptação linguísticas decorrentes dos contextos históricos, de entendimento inafastável ao historiador e ao comparatista, deve obrigatoriamente figurar entre as premissas metodológicas dos que se dedicam a essa tarefa de tradução¹²⁸.

Ciente dessas questões, há como se utilizar dessas compreensões acerca das tradições e traduções jurídicas para se entender, no tempo presente, tentativas recentes de “transplantes” jurídicos? Sabe-se que a influência alienígena no ordenamento jurídico brasileiro, em sua produção legislativa, não é nova¹²⁹. Em tempos recentes, chama a atenção a ingerência realizada, justamente, pela normativa europeia para proteção da privacidade e dos dados pessoais, o Regulamento (UE) 2016/679, denominado de Regulamento Geral de Proteção de Dados, sobre o ordenamento jurídico pátrio, no qual gestou-se a Lei nº 13.709/2018, denominada de Lei Geral de Proteção de Dados.

Com efeito, o transplante que se intenta com a internalização de diversos ditames da RGPD pela LGPD, a fim de satisfazer o requisito europeu de adequação, esbarra, entre outros, na (in)capacidade de os juristas interpretarem, de maneira diversa, os textos normativos, criando normas mais ou menos adequadas à tutela das

¹²⁸ FONSECA, 2020, p. 9.

¹²⁹ Nesse sentido, a pressão britânica ao Brasil quando da formulação e implementação do Bill Aberdeen, em 1845, que culminou com a promulgação da Lei Eusébio de Queiroz, em 1850 (nesse sentido, RÉ, 2019). Em tempos mais recentes, o denominado “Consenso de Washington”, gestado em 1989, talvez seja o exemplo mais representativo desse *lobby* estrangeiro na feitura de leis, de caráter econômico, no Brasil. Sobre a questão verificar: Lima (2002).

brasileiras e brasileiros, e mais ou menos adequadas às exigências do mercado situado nos países centrais, que se beneficiam da captura e tratamento de dados pessoais.

A similitude das legislações é ocasionada, portanto, ao fim e ao cabo, pela inspiração ou pela submissão brasileira à normativa europeia? A melhor interpretação conduz a uma resposta mista – ainda que não totalmente equilibrada. Ora como inspiração, muito como submissão, colmatou-se a legislação brasileira naquele momento histórico e com o texto normativo adquirido ao final do processo legislativo não com a finalidade precípua de bem tutelar o direito à proteção dos dados pessoais dos nacionais brasileiros, mas a fim de se satisfazer a exigência europeia de uma normativa a ela adequada, para não embaraçar os interesses econômicos daqueles que precisam compartilhar dados com empresas situadas em solo Europeu.

O trânsito internacional de dados pessoais permitido pelas atuais tecnologias da informação – o que também faz transitar conceitos jurídicos e termos técnicos – e a inspiração e submissão da lei brasileira à europeia autoriza que chamemos a LGPD de uma tentativa de tradução do RGPD? Em alguma medida, não resta dúvidas de que a lei brasileira tenta traduzir o regramento europeu, a ele adequando o sistema normativo nacional. Nesse aspecto, ao intentar traduzir o que deseja a Europa, e o que se faz presente na normativa europeia, o arcabouço brasileiro, ao ter de, em algum momento, lidar com a realidade nacional, verificará a assimetria que existe entre cada um dos mundos. Nesse ponto se desnudará mais do que a tentativa clara de tradução, compreendida como o transplante legal, que se operou com a feitura da LGPD; ficará claro, como se tem revelado já em tempo recente, a traição do texto original: ou na perspectiva do intérprete, que terá de dá-lo significado distinto do atribuído pelos órgãos julgadores e intérpretes europeus, ou na perspectiva do povo, traído por aqueles capazes de protegê-lo por meio da escuridão prestação jurisdicional ou dispensação dos expedientes previstos pelo Direito, mais preocupados com a submissão ao que deseja a extraterritorialidade.

Exemplo claro do que se afirma é o que se deduz da redação empregada ao art. 10 da Resolução CD/ANPD nº 19/2024. Consonante se verá de forma pormenorizada, a Lei Geral de Proteção de Dados brasileira, em muitos e muitos momentos, se mostra adepta do Regulamento Geral de Proteção de Dados europeu,

com vistas a se me mostrar adequada à Comissão (ou Comitê) Europeu para dele receber o devido selo de país com nível de proteção adequado ao esperado do bloco político e econômico do norte global. No entanto, no momento de afirmar sua posição de soberania e busca por uma tutela efetiva de seus nacionais, falha a Autoridade Nacional de Proteção de Dados brasileira, ao trair o texto e as expectativas dessa suposta “inspiração” (ou submissão?) aos interesses econômicos exógenos, já que faculty, ao talante da ANPD, a averiguação do nível de proteção de dados de países terceiros – com a capacidade de deles exigir salvaguardas adequadas aos interesses nacionais – sem se obrigar, no entanto, a tal. Como se disponíveis fossem os direitos das cidadãs e cidadãos brasileiros no que respeita à proteção que envolve a transferência internacional de seus dados pessoais.

Antes de se lançar totalmente a essa análise, se faz necessário o aprofundamento, assim como realizado no presente capítulo, de conceitos importantes para a responsável compreensão de um contexto maior, que impacta, sobremaneira, a decisão de se obrigar, ou não, uma Autoridade Nacional de Proteção de Dados a analisar o regime normativo de países estrangeiros receptores de dados pessoais de brasileiras e brasileiros.

Se no presente capítulo foi dedicado parte para análise da importância da democracia e da proteção de dados pessoais como princípio constitucional democrático, deve-se, em capítulo apartado, indicar, outrossim, como o poder da privacidade, as exigências do neoliberalismo e a prática do colonialismo de dados influenciam, diuturna e intensamente, a realidade nacional, para então termos consciência de que a proteção de dados pessoais deve envolver uma postura intransigente das autoridades brasileiras na tutela das transferências internacionais de dados pessoais – algo que, atualmente, serve mais a interesses estrangeiros e de grandes capitais nacionais do que às expectativas das brasileiras e brasileiros comuns.

3 O PODER DA PRIVACIDADE, O NEOLIBERALISMO E O COLONIALISMO DE DADOS

3.1 O poder da privacidade e dos dados pessoais na era da informação

O amianto, a par de suas reconhecidas qualidades como matéria-prima para construção de artefatos úteis à indústria de construção civil, – o que lhe garantiu, inclusive, por muito tempo, a alcunha de “mineral mágico”¹³⁰ – traz consigo um grande defeito: ao se comportar como um agente cancerígeno e causador de graves doenças pulmonares, é mortal aos seres humanos.

Os dados pessoais, assim como o amianto, são um ativo tóxico. Sua alta susceptibilidade ao mau uso, e os danos vultosos que acarreta ao serem empregados por entes públicos e particulares para fins antidemocráticos superam, em demasia, os benefícios que hoje vivenciamos ao concedê-los.

A comparação e o exemplo não são inéditos; em verdade, são extraídos da obra *Privacidade é Poder* (2021), de Carissa Véliz. Por meio dessa obra, a filósofa mexicana, professora associada na Faculdade de Filosofia e do Instituto de Ética em Inteligência Artificial do Hertford College, da Universidade de Oxford¹³¹, e conhecida por seu trabalho no campo da privacidade digital e da ética da tecnologia, explora a importância da privacidade em um mundo cada vez mais digitalizado, e argumenta que a privacidade é essencial para a proteção dos direitos humanos e da democracia.

Mas qual a pertinência do exemplo oferecido por Carissa¹³²? A partir dele, a autora traça um paralelo com a atividade voltada à mineração de dados pessoais: seu custo é baixo, sua utilidade é elevada – podem ser empregados com diferentes finalidades, como o de vigiar pessoas, prever comportamentos, e moldar estratégias políticas, comerciais e militares, além de configurarem, em si, um importante ativo comercializável – e, assim como o amianto, os dados pessoais são tóxicos. Nas

¹³⁰Nesse sentido, ver: GOV.BR. Ministério da Saúde. **Amianto**: a exposição ao amianto está relacionada à ocorrência de diversas doenças, sobretudo mesotelioma. Disponível em: <https://www.gov.br/inca/pt-br/assuntos/causas-e-prevencao-do-cancer/exposicao-no-trabalho-e-no-ambiente/amianto>. Acesso em: 15 set. 2023.

¹³¹ VÉLIZ, Carissa. University of Oxford. Institute for Ethics in AI. University of Oxford. Disponível em: <https://www.carissaveliz.com/>. Acesso em: 15 set. 2023.

¹³² Utiliza-se o primeiro nome da autora, porquanto assim referida em seu perfil mantido no site da Universidade de Oxford. Nesse sentido: <https://www.hertford.ox.ac.uk/staff/carissa-veliz>. Acesso em: 15 set. 2023.

palavras de Carissa: *eles podem envenenar vidas humanas, instituições e sociedades*. (VÉLIZ, 2021, p. 129).

Ao se reproduzir um exemplo extraído de obra pensada por alguém que se situa fora do âmbito nacional, e mesmo latino-americano¹³³, não se pretende cometer as mesmas imprecisões criticadas na abertura do trabalho; ao revés, o exemplo oferecido pela autora, além de perspicaz, se mostra adequado à realidade nacional. Isso porque o Supremo Tribunal Federal, em decisão recente, pacificou o tema que há anos enfrentava: a proibição do emprego do amianto, uma vez que, apesar dos aspectos positivos que ostenta, não se justificam quando comparados aos malefícios dele advindos¹³⁴.

¹³³ Talvez o fato de a autora ter nascido no México a tenha sensibilizado para pensar o aspecto da privacidade não somente na ótica do centro – mormente os Estados Unidos e os países do oeste da Europa. O histórico de perseguição sofrido por seus familiares também pode funcionar como um indício do que move a filósofa às reflexões colocadas em seu livro. Com efeito, assim foi sobre ela noticiado: *“Nacida en México en el seno de una familia española que tuvo que salir de España después de la guerra civil y que encontró refugio en ese país, Véliz empezó a interesarse por la privacidad cuando se puso a investigar la historia de sus familiares en archivos en España”*. BBC News Mundo. **La falta de privacidad apoya un sistema económico inmoral, asegura filósofa mexicana**. Disponível em: <https://abrir.link/Ra1HS>. Acesso em: 15 set. 2023.

¹³⁴ Em 2017, o Supremo Tribunal Federal (STF) emitiu decisões relevantes relacionadas à regulamentação do uso do amianto crisotila no Brasil. O STF considerou válidas cinco leis estaduais e uma municipal que impunham restrições ou proibições à extração e ao uso do amianto crisotila na produção de diversos materiais. Ao mesmo tempo, a mais alta corte brasileira declarou a inconstitucionalidade de uma lei federal que autorizava a extração, industrialização, comercialização e distribuição dessa fibra mineral no país. Essas decisões foram fundamentadas na comprovação científica da natureza cancerígena do amianto e na inviabilidade de seu uso seguro, bem como na existência de alternativas viáveis para a matéria-prima em questão. O julgamento envolveu várias Ações Diretas de Inconstitucionalidade (ADIs) e uma Arguição de Descumprimento de Preceito Fundamental (ADPF). A Confederação Nacional dos Trabalhadores da Indústria (CNTI) apresentou as ADIs 3356, 3357, 3937, 3406 e 3470, contestando leis restritivas dos estados de Pernambuco, Rio Grande do Sul, São Paulo, Rio de Janeiro e do município de São Paulo. Argumentava-se que as legislações estaduais e municipais estavam em conflito com a legislação federal sobre o tema. Além disso, a Associação Nacional dos Magistrados da Justiça do Trabalho (Anamatra) questionou a lei federal que permitia o uso do amianto crisotila na ADI 4066. O STF entendeu que o artigo 2º da Lei federal 9.055/1995 passou por um processo de “institucionalização” devido à evolução das informações sobre os riscos do amianto crisotila à saúde e ao meio ambiente. Embora a lei tenha sido promulgada quando já havia preocupações sobre os riscos, o consenso posterior sobre a natureza altamente cancerígena do mineral tornou-a incompatível com a Constituição Federal. Organizações nacionais e internacionais especializadas em saúde pública e saúde ocupacional também concluíram que o uso seguro do amianto era inviável. A ministra Rosa Weber, relatora de várias dessas ações, enfatizou o consenso científico sobre os danos à saúde causados pela exposição ao amianto. Ela argumentou que não era razoável admitir a compatibilidade dessa substância com a Constituição, dada a proteção constitucional à saúde e ao meio ambiente. Além disso, mencionou a Convenção 162 da Organização Internacional do Trabalho (OIT), que tratava do banimento do amianto e recomendava sua substituição progressiva por alternativas mais seguras. Em fevereiro de 2023, o STF concluiu o julgamento de recursos relacionados à proibição da exploração do amianto crisotila e confirmou a declaração de inconstitucionalidade da norma federal sobre o assunto. É importante observar que, por uma questão de quórum, a lei federal que permitia o uso do amianto não foi declarada inconstitucional em um dos julgamentos, a ADI 4066. No entanto, a inconstitucionalidade das leis estaduais foi

Antes de se explorar, em profundidade, o pensamento de Carissa Véliz, duas questões, de pronto, devem ser confrontadas. A primeira corresponde a uma possível afirmação, decorrente do senso comum moderno, de que os meios e os fins são independentes entre si. No caso dos dados pessoais, significaria afirmar que a mera concessão desses dados, ou seja, sua simples captação pelos diversos atores e dispositivos não importaria, necessariamente, um uso deturpado deles enquanto matéria prima, porquanto dependeria, ao fim e ao cabo, do tratamento e destinação que a eles seria dado – um exemplo paralelo, mas que bem ilustra o que se quer afirmar, corresponde à afirmação, não raramente ouvida, de que “as armas não matam pessoas, as pessoas é que matam pessoas”¹³⁵.

Tal visão meramente instrumentalista da tecnologia veria, nos artefatos por ela produzidos, um suporte neutro e livre de valores, porquanto não intrinsecamente destinados a cumprir esse ou aquele objetivo, mas suscetíveis ao desejo humano daqueles que os utilizariam. Essa não é a visão adotada nessa obra; com efeito, tanto a arquitetura externa quanto interna dos artefatos tecnológicos cumprem funções pensadas por aqueles responsáveis pela sua concepção e construção. Tais funções são limitadas, efetivamente, pela imperiosa prestabilidade dos dispositivos (um objeto tecnológico concebido de maneira imprestável, ou seja, que não funcione para os fins que anunciadamente se destina, a nada serve enquanto técnica), mas também carregam consigo aspectos socialmente delineados; ou seja, no mais das vezes, poderiam ser construídos e configurados desse ou de outro jeito – razão pela qual a maneira como operam, com maior ou menor propensão à ofensa ou proteção de

declarada de forma incidental nas outras ADIs. Essas decisões do STF refletem um compromisso com os objetivos de desenvolvimento sustentável, particularmente os relacionados ao consumo e produção responsáveis, a ação contra as mudanças climáticas, a proteção da vida aquática e terrestre, de acordo com a Agenda 2030 da Organização das Nações Unidas (ONU). Para mais detalhes sobre as decisões do STF, é possível consultar os acórdãos completos das ADIs e da ADPF mencionadas. SUPREMO TRIBUNAL FEDERAL. **Especial Meio Ambiente**: STF proíbe extração e venda de amianto crisotila. Disponível em: <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=509089&ori=1>. Acesso em: 15 set. 2023.

¹³⁵ “Para o senso comum moderno, os meios e os fins são independentes entre si. Um exemplo: na América dizemos “as armas não matam pessoas, as pessoas é que matam pessoas”. As armas são um meio que é independente dos fins que lhe dá o utilizador, quer seja roubar um banco ou aplicar a lei. Dizemos que a tecnologia é neutra, significando que não tem preferência entre os vários usos possíveis em que é posta em uso. Esta é a filosofia instrumentalista da tecnologia, que é uma espécie de produto espontâneo da nossa civilização, e assumida irrefletidamente por muita gente”. (FEENBERG, 2015, p. 124).

direitos, com pendor, *v.g.*, à proteger ou atacar bens jurídicos, depende, não raro, da intencionalidade daqueles que os concebem¹³⁶.

A outra questão corresponde aos claros benefícios que vivenciamos na atualidade, decorrentes do largo emprego da tecnologia. São tantos que enumerá-los nos conduziria, inexoravelmente, a um rol exemplificativo. Isso também decorre da amplitude que evolui do próprio conceito de tecnologia¹³⁷ e, por conseguinte, do de dispositivos tecnológicos; no entanto, a mera vivência e experiência contemporânea são capazes de nos fornecerem uma profusão de exemplos: o diuturno e instantâneo contato com parentes e amigos por meio de aplicativos de mensagens e chamadas de áudio e de vídeo, independente de distâncias geográficas (mas não de sinal de internet); a realização de operações bancárias de forma remota; a marcação de consultas médicas e compromissos profissionais sem a dependência do horário

¹³⁶ Retoma-se, nesse aspecto, o determinismo tecnológico criticado por Andrew Feenberg, em exemplo emblemático por ele consignado, acerca da correlação entre a tecnologia e o trabalho infantil na Inglaterra. Nesse sentido, discorre que: “consideremos a notável antecipação das atitudes atuais nos movimentos de luta sobre a extensão do trabalho diário e sobre a mão-de-obra infantil, em meados do século XIX, na Inglaterra. Os debates sobre a lei fabril de 1844 foram inteiramente estruturados em torno da oposição entre imperativos tecnológicos e ideologia. Lord Ashley, o principal líder a favor da regulamentação, protestou que “a tendência para os vários aperfeiçoamentos das máquinas caminha no sentido de substituir o emprego de homens adultos e de colocar o trabalho de crianças e mulheres no seu lugar. Qual será o efeito sobre as gerações futuras se a sua frágil constituição ficar subordinada, sem limitações ou controle, a essas ações destrutivas?” (2017, p. 84).

¹³⁷ Alberto Cupani bem discorre sobre o conceito polissêmico do termo “tecnologia”, ao ensinar que “Aquilo que denominamos tecnologia se apresenta, pois, como uma realidade polifacetada: não apenas em forma de objetos e conjuntos de objetos, mas também como sistemas, como processos, como modos de proceder, como certa mentalidade. A essa presença múltipla devemos acrescentar uma patente ambiguidade daquilo a que aludimos como tecnologia. Invariavelmente, toda realização tecnológica vai acompanhada de alguma valoração, positiva ou negativa. Em certos casos, como no das armas de destruição em massa ou da poluição ambiental resultante da industrialização, consideramo-las como algo condenável, que desejaríamos não existisse. Em outros, como no das vacinas, do transporte confortável ou do cinema, a maioria das pessoas vê nessas realizações algo que veio beneficiar a espécie humana. Mas a propósito da maior parte dos objetos e processos tecnológicos há lugar para a dissensão, permanente ou circunstancial” (2016, p. 12). Em sentido parecido, também Andrew Feenberg: “A tecnologia não pode continuar a ser considerada nem como uma coleção de dispositivos nem, de um modo mais geral, como a soma de meios racionais. Essas são definições tendenciosas suscitam a questão da significância social e dos envolvimento da tecnologia. Enquanto objeto social, a tecnologia precisa de estar sujeita a uma interpretação, como qualquer outro artefato cultural, mas geralmente é excluída das ciências humanas. Asseguram-nos que a sua essência reside numa função tecnicamente explicável, em vez de um significado interpretável por via hermenêutica. No máximo, os métodos das ciências humanas apenas podem trazer alguma luz aos aspetos extrínsecos da tecnologia, como a questão das embalagens e da publicidade, ou às reações populares às inovações consideradas controversas, como a energia nuclear. O determinismo tecnológico extrai a sua força a partir dessa atitude. Se ignorarmos a maioria das ligações entre tecnologia e sociedade, não é surpresa que a tecnologia nos possa aparecer como algo gerador de si próprio” (2017, p. 87).

comercial e de um atendente humano; o acesso a documentos pessoais outrora válidos apenas se portados em seu formato físico, entre vários outros.

Não há o que se discutir sobre os proveitos decorrentes do avanço tecnológico. O que emerge desse questionamento é: e os efeitos deletérios? São intrínsecos a esse avanço? Levando-se também em conta esses prejuízos, a conformação tecnológica (o atual “estado da arte”) não poderia ser diferente, e, quem sabe, se não idêntico, tão proveitoso quanto? E, para o que nos interessa enquanto objeto principal de reflexão, a concepção leve e pesada dos dispositivos atuais não poderia ser feita sem intencionar a massiva coleta e tratamento de dados pessoais? Ao fim e ao cabo, em um mundo hiperconectado e dependente das modernas tecnologias de informação e comunicação, há espaço para uma concepção capaz de proteger a privacidade das atividades de transferência internacional de dados pessoais?

A resposta adotada no trabalho é positiva, e perpassa por uma compreensão crítica da tecnologia. Tal compreensão encontra eco, justamente, nas principais reflexões apresentadas por Carissa Véliz; no entanto, antes de discuti-las, na medida que invocamos o termo “privacidade”, e considerando os dados pessoais como conexos, mas não idênticos, aos sentidos atribuídos a esse vocábulo, necessário também se faz uma abordagem, por mais que não exaustiva, do que usualmente denomina.

A verdadeira complexidade da questão da privacidade não reside apenas na definição semântica¹³⁸ do termo, mas sim na necessidade de construir uma metalinguagem adequada para abordar esse conceito. Conforme apontado por Danilo Doneda, a privacidade muitas vezes é usada para atender a necessidades estruturais

¹³⁸ O próprio termo “privacidade” comporta certa polissemia em sua significação lexicográfica, oscilando ora entre as noções circundantes à “intimidade da vida”, ora mais próximo de um sentido de “confidencialidade”. Nesse contexto, é definido pelo linguista Aurélio Buarque de Holanda como verbete derivado de um anglicismo (*privacy*), cujo significado remeteria à “*vida privada, vida íntima, intimidade*” (FERREIRA, 1986. p. 1394). Privado, por sua vez, é definido pelo linguista como algo que “*não é público; particular*”. Por fim, o termo privar é definido como “*conviver intimamente, ser íntimo*”. Outro linguista, Antonio Houaiss, define como sinônimos do termo Privacidade os vocábulos “*intimidade, privatividade, vida íntima*”. Privado, por sua vez, ostenta os sinônimos “*confidencial, reservado, secreto, sigiloso*” (HOUAISS, 2003, p. 536).

específicas, assumindo diferentes significados de acordo com o contexto legal¹³⁹, o que dificulta sua redução a um único sentido comum (DONEDA, 2006, p. 103).

Doneda sugere que, em vez de se concentrar exclusivamente na definição da privacidade, é essencial compreender o que se espera dessa definição¹⁴⁰. Ele argumenta que uma abordagem eficaz envolve traçar um panorama abrangente da esfera privada da pessoa, levando em consideração fatores sociais, culturais e políticos que a influenciam¹⁴¹.

Nesse contexto, Marcel Leonardi destaca quatro teorias que buscam conceituar a privacidade de forma unitária: o direito a ser deixado só¹⁴², a proteção

¹³⁹ No mesmo sentido Marcel Leonardi, ao afirmar que a expressão “privacidade” tornou-se uma “palavra-camaleão” (...). In: LEONARDI, 2011, p. 46.

¹⁴⁰ O que significa se indagar que tipo de definição apresentará naquele contexto linguístico específico, o que se remete às questões outrora trabalhadas, referentes à importância dos “jogos de linguagem” na construção e compreensão dos conceitos.

¹⁴¹ Em pese tenha Danilo Doneda intuído sobre a necessidade de se considerar os fatores sociais e culturais no que tange à própria definição da privacidade e, por conseguinte, de sua proteção, não avançou a um delineamento mais profundo do que isso consistiria ao se ter em conta a posição brasileira como colônia digital dos países de centro.

¹⁴² Muitas vezes referenciado com o termo original em inglês – *the right to be let alone* – esse contorno do direito à privacidade vem sendo debatido, há mais de um século, nos Estados Unidos, tendo o seu reconhecimento, principalmente, a partir da atividade da Suprema Corte. Denominado, em seu viés jurídico-protetivo, de *right to privacy*, a gênese moderna desse direito está ligada a um artigo escrito, no ano de 1890, pelos juristas Samuel Warren e Louis Brandeis, publicado na revista *Harvard Law Review*, denominado *The right to privacy*. Por meio desse escrito, os juristas criticaram a invasão da privacidade social pela imprensa da época, com a exposição, em público, de fatos privados. Transcreve-se, por oportuno, pequeno excerto do artigo, em que justificam tal perspectiva: “Fotografias instantâneas e empresas de jornais invadiram os recintos sagrados da vida privada e doméstica; e inúmeros dispositivos mecânicos ameaçam confirmar a previsão de que “o que é sussurrado no armário será proclamado do alto da casa”. Durante anos tem havido um sentimento que a lei deve propor algum remédio para a circulação não autorizada de retratos de pessoas privadas; E o mal da invasão da privacidade pelos jornais, há muito sentida, tem sido discutida recentemente [...]” (WARREN; BRANDEIS, 1890, p. 195). Original em inglês: *Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that “what is whispered in the closet shall be proclaimed from the house-tops.” For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers, long keenly felt, has been but recently discussed [...]*(idem). Não que a privacidade não tivesse sido, antes, mencionada em âmbito norte-americano: o mérito desse artigo é o de deslocar o âmago da proteção conferida pela *privacy* de uma perspectiva privatista, ligada à propriedade, para um caráter pessoal, em viés constitucional. Além disso, bem representa o sentimento social, político e econômico vivido naquele contexto, em que era efervescente a disseminação da comunicação em novas plataformas, à época, consideradas tecnológicas. Não deve, entretanto, se confundir com a moderna concepção de privacidade e de dados pessoais, visto que, a cada época, a própria necessidade de um conceito de privacidade obedece a necessidades distintas. Nesse sentido, Danilo Doneda: “O artigo é inédito ao propor uma força inédita ao novo *right to privacy*, e também é mais que mero reflexo de uma época, fazendo estender sua influência por algumas de suas características: (i) partia-se de um novo fato social, que eram as mudanças trazidas para a sociedade pelas tecnologias da informação (jornais, fotografias) e a comunicação de massa, fenômeno que se renova e continua moldando a sociedade futura; (ii) o novo “direito à privacidade” era de natureza pessoal, e não se aproveitava da estrutura da tutela da propriedade para proteger aspectos da privacidade; (iii) no que

contra interferências de terceiros, a preservação de segredos ou informações confidenciais e o controle sobre informações e dados pessoais. Embora todas essas teorias sejam relevantes para a compreensão da privacidade, Leonardi argumenta que uma abordagem exclusiva baseada em informações e dados pessoais pode ser limitada, uma vez que exclui aspectos privados que não estão relacionados a tais informações¹⁴³. Ele enfatiza que a privacidade não é, portanto, apenas uma prerrogativa individual subjetiva, e nem se resume, unicamente, aos dados pessoais, mas abrange o que a sociedade considera, em todos esses aspectos, adequado proteger¹⁴⁴.

Há, portanto, algum consenso entre os estudiosos de que a privacidade requer uma definição ampla e pluralista para se adequar à realidade do ser humano¹⁴⁵. Isso ocorre porque a proteção da privacidade está intrinsecamente ligada à dignidade da pessoa humana e envolve a capacidade de se controlar informações pessoais, bem como a construção de uma esfera pessoal na qual as pessoas têm liberdade de escolha e desenvolvimento de sua própria personalidade. Nesse sentido, a privacidade não é um conceito finalista, mas sim um instrumento para proteger a dignidade das pessoas.

Ao se insistir na pluralidade do conceito de privacidade, o que se objetiva, verdadeiramente, é posicioná-lo e distingui-lo em um universo semântico que habita em companhia do sentido dado aos “dados pessoais”. Isso porque, ainda que teorias unitárias tendam a confundir-los, identificando-os plenamente um com o outro, não há

interessa somente aos EUA, o artigo abriu caminho para o reconhecimento (que porém ainda tardaria décadas) do direito à privacidade como um direito constitucionalmente garantido” (DONEDA, 2006, p. 139).

¹⁴³ Leonardi não adota, assim, qualquer dessas teorias unitárias, mas antes as condensa, a fim de criar um conceito pluralista de privacidade. Nesse sentido afirma, inclusive, que “a insistência em isolar as características essenciais da privacidade e reuni-las em um conceito unitário, aplicável indistintamente em quaisquer situações, é tarefa que tende a fracassar” (LEONARDI, 2011, p. 51).

¹⁴⁴ Assim como Doneda, compreende-se que Leonardi, apesar de ter bem intuído a questão, não avançou a um delineamento mais autônomo e autêntico no que toca às pretensões brasileiras.

¹⁴⁵ Além de Doneda (2006) e Leonardi (2011), poderíamos elencar as conceituações apresentadas por Tatiana Malta Vieira, ao lecionar que: “buscando um conceito abrangente, o direito à privacidade consistiria em um direito subjetivo de toda pessoa – brasileira ou estrangeira, residente ou transeunte, física ou jurídica – não apenas de constranger os outros a respeitarem sua esfera privada, mas também de controlar suas informações de caráter pessoal – sejam estas sensíveis ou não – resistindo às intromissões indevidas provenientes de terceiros” (VIEIRA, 2007, p. 23); e por João Carlos Zanon, para quem “é possível identificar, entretanto, em todos os sentidos atribuídos ao direito à privacidade certo consenso, que corresponderia a ter por característica básica a pretensão de estar separado de grupos, mantendo o indivíduo livre da observação de outros” (ZANON, 2013, p. 36) .

como considerá-los amalgamados; enquanto a privacidade comporta aspectos distintos do expresso pelos dados pessoais, esses se sobrepõem no contexto contemporâneo, ultrapassando o caráter privado das outras definições de privacidade mais voltadas à proteção individual contra ingerências alheias em questões íntimas e pessoais, para denotar como o esquadramento social provoca efeitos deletérios supraindividuais, atingindo, em verdade, os mais caros valores coletivos, entre eles, o da democracia.

Desse modo, também é da pluralidade que advém a marca distintiva dos conceitos. Ao nos referirmos à “privacidade”, o que se sobrepõe é o aspecto pessoal e privado do instituto, vinculado à noção de um direito individual estático, de um ser humano que se deseja se opor, em sua esfera íntima, a todos os outros; quando mencionados, porém, os dados pessoais, destacamos, a partir do que leciona Stefano Rodotà, a dinamicidade do conceito, voltado ao exercício do direito à igualdade perante a coletividade¹⁴⁶.

Com essa distinção não se afirma, entretanto, que a informação contida em dados pessoais não possa revelar aspectos da privacidade que dizem respeito a componentes individuais do sujeito. Nem quer se afirmar que tal conteúdo detenha valor diminuído para o titular dos dados pessoais. Ao revés. A exposição da privacidade, seja ela veiculada diretamente por mídias fotográficas ou videográficas, seja por meio de informações obtidas a partir de dados pessoais, costuma causar ao lesado intenso sofrimento, visto que desnudado em sua esfera íntima, cuja participação não é dada à sociedade em geral.

Os dados pessoais, em alguma medida, levam em consideração, quando não englobam, o instituto da privacidade. Essa é a razão pela qual certos autores afirmam ser a tutela dos dados pessoais uma evolução do próprio conceito de privacidade¹⁴⁷. Sem adentrar nessa discussão, afirma-se apenas que o direito à proteção dos dados

¹⁴⁶ Nesse sentido escreve o jurista italiano: “o direito ao respeito da vida familiar reflete, primeira e principalmente, um componente individualista: este poder basicamente consiste em impedir a interferência na vida privada e familiar de uma pessoa. Em outras palavras, é um tipo de proteção estático, negativo. Contrariamente, a proteção de dados estabelece regras sobre os mecanismos de processamento de dados e estabelece a legitimidade para a tomada de medidas – i.e. é um tipo de proteção dinâmico, que segue o dado em todos os seus movimentos” (RODOTÁ, 2008, P. 17).

¹⁴⁷ Nesse sentido, Danilo Doneda: “A necessidade de funcionalização da proteção da privacidade fez, portanto, com que ela originasse uma disciplina de proteção de dados pessoais, que compreende pressupostos ontológicos idênticos aos da própria proteção da privacidade: pode-se dizer que é a sua “continuação por outros meios”. (DONEDA, 2006, p. 27).

peçoais, frente toda essa complexidade até agora apresentada, é autônomo e específico dos demais concernentes à matéria, merecendo, em razão disso, consideração especial e apartada¹⁴⁸.

O direito à proteção de dados pessoais possui, nesse contexto, objeto próprio¹⁴⁹: a tutela das informações relativas a indivíduo específico ou especificável. O valor subjacente à norma, por sua vez, diz respeito à proteção do próprio indivíduo e de sua dignidade contra ingerências não democráticas em sua existência, mormente àquelas destinadas a ferir o princípio da igualdade que sustenta, em larga medida, o diploma constitucional em vigor no Brasil¹⁵⁰ - de tal modo que os reflexos de uma atividade discriminatória no bojo da sociedade podem acarretar efeitos devastadores para a paz social, podendo se desdobrar sobre agrupamentos sociais inteiros.

Em sua perspectiva estática ou dinâmica, portanto, os dados pessoais revelam que seu intrincado delineamento e a prodigalidade com que se espraiam em diferentes e relevantes aspectos da vida individual e coletiva dos indivíduos apenas reforçam a acuidade com que Carissa Véliz expõe a questão da privacidade: a compreendendo, justamente, em sua complexidade, e dedicando momentos específicos para tratar de diferentes temas com as nuances necessárias, à exemplo do que faz em tópico dedicado à toxicidade dos dados pessoais.

¹⁴⁸ Sobre a questão o escólio de João Carlos Zanon: “Os bens jurídicos tutelados pela privacidade e pelo direito à proteção dos dados pessoais não são coincidentes. Na privacidade, tutela-se a integridade psíquica do indivíduo (a necessidade humana de ter para si uma esfera de reserva). A proteção dos dados pessoais resguarda a pessoa de não ser discriminada pelas suas crenças religiosas, suas opiniões políticas e filosóficas, por sua etnia, condições de saúde ou orientação sexual; proteger os dados pessoais significa, também, evitar que o indivíduo seja impedido de acessar bens e serviços, a princípio só oferecidos àqueles com bons credenciais; conferir proteção aos dados pessoais implica, ainda, livrar-se de etiquetas e chancelas. Portanto, com a proteção aos dados pessoais, busca-se, sobretudo, a não discriminação, a não exclusão e a promoção da liberdade”. (ZANON, 2013, p. 151).

¹⁴⁹ No Brasil, a Lei Geral de Proteção de Dados (LGPD) conceitua “dado pessoal” da seguinte forma: “Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável”.

¹⁵⁰ Nesse sentido, novamente Stefano Rodotà: De fato, coletar dados sensíveis e perfis sociais e individuais pode levar à discriminação; logo, a privacidade deve ser vista como “a proteção de escolhas de vida contra qualquer forma de controle público e estigma social” (L. M. Friedman), como a “reivindicação dos limites que protegem o direito de cada indivíduo a não ser simplificado, objetivado, e avaliado fora de contexto” (J. Rosen). Já que os fluxos de informação não contêm somente dados “destinados para fora” – a serem mantidos longe das mãos alheias –, mas também dados “destinados para dentro” – sobre os quais talvez a pessoa queira exercer o “direito de não saber” –, a privacidade deve ser considerada também como o “direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular. Ao reivindicar a autonomia do indivíduo na sociedade da informação, uma decisão histórica da Corte Constitucional Alemã de 1893 reconheceu a “autodeterminação informativa” (RODOTÀ, 2008, p. 15).

Nesse contexto, o primeiro aspecto da toxicidade dos dados pessoais enfocado pela autora é o que chama de “vidas envenenadas”. Nesse sentido, enfatiza como as pessoas, individualmente consideradas, são afetadas pela coleta, tratamento e emprego de dados pessoais pelas empresas atuantes no mundo digital – em verdade, não apenas pelas empresas, mas também pelo Estado, mormente em suas atividades vinculadas ao privilégio que lhe foi concedido em sua passagem à modernidade: o monopólio da violência legítima.

Cientes de que a segurança dos dados pessoais é uma questão crucial nos tempos modernos, com o potencial de afetar profundamente a vida das pessoas, as reflexões propostas por Carissa revelam que, quando essas informações caem em mãos erradas, os resultados podem ser devastadores¹⁵¹, e a recuperação é quase impossível (VÉLIZ, 2021, p. 131). Nesse contexto, a verdade é que qualquer pessoa pode ser afetada, mesmo que não tenha segredos obscuros. Dados aparentemente mundanos, como passaportes, carteiras de identidade, nomes, endereços e informações bancárias, podem ser alvos de ataques e causar estragos na vida de seres humanos¹⁵². A pesquisa apresentada por Carissa indica que a maioria das pessoas experimentou alguma forma de violação de privacidade online, desde roubo de identidade até humilhação pública e problemas com softwares espões¹⁵³.

¹⁵¹ Um exemplo impactante dessa realidade ocorreu em 18 de agosto de 2015, quando mais de 30 milhões de indivíduos tiveram seus dados pessoais expostos na internet. Hackers divulgaram o banco de dados completo dos clientes do Ashley Madison, um site de encontros que facilitava casos extraconjugais. Os dados incluíam nomes, endereços, preferências, códigos postais e números de cartão de crédito dos usuários, incluindo aqueles que haviam cancelado suas inscrições. O propósito dos hackers era punir os infiéis, uma motivação moralmente questionável

¹⁵² Um exemplo de roubo de identidade ocorreu com Ramona María Faghiura, na Espanha, em janeiro de 2015. A vítima foi acordada por dois homens, que a detiveram com base em um mandado de prisão. Mesmo afirmando sua inocência e que era vítima de roubo de identidade, Ramona foi presa e passou anos lidando com o sistema de justiça espanhol, gastando grandes quantias de dinheiro em advogados e enfrentando graves problemas psicológicos. Sua vida foi profundamente afetada, embora ela não tivesse cometido crime algum. Diferentemente do caso anterior, o de Ramona María Faghiura não obteve, das mídias brasileiras, qualquer atenção. Tanto é que se reproduz, para consulta, a mesma matéria jornalística indicada por Carissa Véliz (VÉLIZ, 2021, p. 132), ante a ausência de matérias, em português, sobre o caso: EL PAÍS. “**Me han robado la identidad y estoy a base de lexatín; yo no soy una delincuente**”. Publicado em 24 de agosto de 2016. Disponível em: https://elpais.com/politica/2016/08/23/actualidad/1471908298_138488.html. Acesso em: 20 ago. 2023.

¹⁵³ A pesquisa em questão foi conduzida pela própria Carissa Véliz, em parceria com Siân Brooke (pesquisadora do Departamento de Metodologia da Universidade de Oxford – *Oxford Internet Institute*), e encontra-se hospedada no site: PHILARCHIVE.ORG. **Views on Privacy. a survey**. Disponível em: <https://philarchive.org/rephilarchive.org/BROVOP-3>. Acesso em: 20 ago. 2023. Uma referência na mídia brasileira sobre a pesquisa pode ser encontrada no site: FOLHA DE S. PAULO. **É preciso acabar com o modelo digital baseado nos dados pessoais, diz professora**. Disponível

Outro crime relacionado a dados é a extorsão, que envolve o uso de informações pessoais roubadas para chantagear as vítimas. Um exemplo chocante foi o ataque a uma clínica de cirurgia estética na Lituânia, onde pacientes foram chantageados com a ameaça de revelar fotos privadas e informações pessoais (VÉLIZ, 2021, p. 133).

Esses incidentes destacam a urgência de proteger os dados pessoais em um mundo digital cada vez mais vulnerável. A exposição de informações pessoais pode ter um impacto profundo e devastador na vida das pessoas (singularmente consideradas, e mesmo em seus familiares e demais pertencentes a círculos próximos de trabalho e amizade), e é um desafio que afeta não apenas indivíduos, mas também governos e empresas.

No Brasil, talvez o caso mais célebre de afronta à privacidade e ao direito individual daqueles que expõe dados íntimos em ambientes virtuais seja composto pelos fatos que envolveram a atriz Carolina Dieckmann, vítima de invasão de seus computadores e vazamento de conteúdo pessoal. Editou-se, a partir disso, a Lei Carolina Dieckmann¹⁵⁴, oficialmente conhecida como Lei nº 12.737/2012, que trata da criminalização de invasão de dispositivos informáticos e a divulgação não autorizada de informações privadas na internet, em resposta a um caso de violação de privacidade e divulgação não autorizada de fotos da atriz Carolina Dieckmann. A lei é importante no Brasil porque estabelece medidas legais para lidar com crimes cibernéticos, proteger a privacidade online e responsabilizar aqueles que violam sistemas de computadores e divulgam informações pessoais sem consentimento. Ela tem como objetivo fortalecer a segurança cibernética e garantir a proteção dos dados pessoais, sendo um marco na regulamentação das atividades online no país.

O segundo aspecto da toxicidade dos dados pessoais é chamado de “instituições envenenadas”. A vulnerabilidade dos dados pessoais não se limita apenas aos indivíduos; ela também se estende às instituições que os armazenam e analisam. Qualquer forma de armazenamento de dados pode potencialmente

em:<https://www1.folha.uol.com.br/tec/2021/01/e-preciso-acabar-com-o-modelo-digital-baseado-nos-dados-pessoais-diz-professora.shtml>. Acesso em: 20 ago. 2023.

¹⁵⁴ Há mais de uma década em vigor, a Lei Carolina Dieckmann (Lei n. 12.737/2012) foi aprovada menos de dois anos após a divulgação de imagens íntimas da atriz, que teve seu computador invadido e 36 fotos roubadas, além de sofrer uma tentativa de extorsão. Desde então, invadir computadores, celulares e outros aparelhos é, no Brasil, crime punível com prisão.

desencadear um desastre que afeta negativamente uma empresa, prejudica sua reputação, reduz sua participação de mercado e, em casos extremos, resulta em processos judiciais onerosos ou até mesmo em acusações criminais. Empresas que acumulam mais dados do que o necessário, estão, de certa forma, na forma como vê Carissa Véliz, criando um risco para si mesmas.

Embora algumas empresas tenham conseguido sobreviver a desastres de dados, nem todas têm a mesma sorte. Um exemplo notável é o caso “Ashley Madison”, cuja empresa, apesar do vazamento de dados em larga escala, parece ter economicamente se recuperado – ainda que sua imagem tenha sido danificada, e sua reputação, abalada¹⁵⁵.

Outro exemplo é a Meta, que, apesar de ter sobrevivido a vários escândalos relacionados aos dados dos usuários, enfrentou sérias críticas e perdeu a confiança do público. A empresa pode enfrentar desafios no longo prazo se um concorrente mais ético surgir. Em uma pesquisa recente, a Meta foi classificada como a empresa de tecnologia menos confiável pelos participantes, recebendo uma pontuação extremamente baixa – e, embora a Meta tenha conseguido manter sua posição dominante até agora, sua falta de respeito à privacidade pode eventualmente afetar sua posição no mercado. Consoante salientado pela filósofa mexicana-espanhola, trabalhar na Meta deixou de ser uma fonte de orgulho para muitos de seus funcionários e ex-funcionários (VÉLIZ, 2021, p. 135).

A lição a ser aprendida, conforme a autora, é que, assim como qualquer substância tóxica, o manuseio de dados sensíveis requer precaução e responsabilidade. Quando ocorrem falhas graves, o resultado pode ser a morte de uma empresa. Um exemplo notório é o caso da *Cambridge Analytica*, que entrou em processo de insolvência e encerrou suas operações após a revelação de suas práticas de influência política com dados pessoais de eleitores. Da mesma forma, o Google

¹⁵⁵ Notícias dão conta que, após o vazamento de dados, a empresa demorou, aproximadamente, dois anos para se mostrar, novamente, lucrativa. No entanto, não há rumores de que os problemas vivenciados anos atrás tenham desestimulado o acesso e concessão de dados – e os lucros deles provenientes – para milhões de usuários. Com efeito, durante a pandemia, verificou-se que o número de usuários subiu de 60 milhões para 70 milhões – acréscimo superior a 10% (dez por cento). Nesse sentido: DANA, Samy. Ashley Madison: o que a economia nos diz sobre a traição. **JP News**. <https://jovempan.com.br/arquivo/samy-dana/ashley-madison-o-que-a-economia-nos-diz-sobre-a-traicao.html>. Acesso em: 20 ago. 2023.

encerrou sua rede social, o *Google+*, depois que falhas em seu projeto permitiram que desenvolvedores externos tivessem acesso aos dados pessoais dos usuários.

Mesmo que uma instituição sobreviva a um escândalo de dados, o custo pode ser exorbitante. A Meta, por exemplo, foi multada em bilhões de dólares nos Estados Unidos e no Reino Unido devido a várias violações de privacidade. Com a implementação do Regulamento Geral de Proteção de Dados (RGPD) na Europa, as multas podem chegar a 4% da receita ou 20 milhões de euros, o que for maior¹⁵⁶. Instituições que não mudarem suas práticas enfrentarão multas mais pesadas e frequentes, pois a regulamentação visa alinhar os interesses das empresas com a proteção dos dados dos clientes (*Idem*).

No caso do Brasil, com a Lei Geral de Proteção de Dados (LGPD), as penalidades também são severas. A multa por violação pode atingir até 2% do faturamento da empresa, limitada a R\$ 50 milhões por infração, dependendo da gravidade da situação. Assim como o RGPD na Europa, a LGPD visa garantir que as empresas tratem os dados pessoais de forma segura e responsável¹⁵⁷. A diferença entre os diplomas normativos está no limite máximo das multas, que na LGPD é fixado, mas que ainda assim pode representar uma perda colossal, especialmente para empresas com receita elevada. Isso reforça a importância de políticas rigorosas de conformidade com a lei para evitar prejuízos substanciais.

Em alguns casos, as violações de dados não resultam apenas em multas, mas também causam danos significativos à reputação e à segurança de um país. Um exemplo disso foi o ataque cibernético ao Escritório de Gerenciamento de Pessoal dos Estados Unidos em 2015, que resultou no roubo de milhões de registros sensíveis do governo, incluindo informações sobre funcionários federais. Esse tipo de violação não apenas prejudica a imagem de uma instituição, mas também coloca em risco a segurança nacional (*Ibidem*, p. 136).

¹⁵⁶ Cf. art. 83, RGPD.

¹⁵⁷ Recentemente, a ANPD determinou a suspensão cautelar do tratamento de dados pessoais para treinamento da IA da Meta, estabelecendo multa diária de R\$ 50 mil por eventual descumprimento. GOV.BR. **Diário Oficial da União**. Despacho Decisório nº 20/2024/PR/ANPD. Processo nº 00261.004509/2024-36. Interessado: META PLATFORMS INC - FACEBOOK SERVIÇOS ONLINE DO BRASIL. Disponível em: <https://www.in.gov.br/en/web/dou/-/despacho-decisorio-n-20/2024/pr/anpd-569297245>. Acesso em: 10 jul. 2024.

No Brasil, o caso mais emblemático envolvendo a malversação de dados pessoais por uma empresa privada talvez corresponda ao vazamento de dados de quase 2 milhões de usuários, pela empresa *Netshoes*, no mês de dezembro de 2017¹⁵⁸. O vazamento revelou o nome, data de nascimento, endereço, CPF e informações de pedidos de 1.999.704 contas de clientes. Além disso, o incidente vazou informações de servidores públicos que estavam cadastrados no banco de informações da empresa¹⁵⁹. Para se ver livre de um processo milionário, a empresa de venda de artigos esportivos pela internet firmou um Termo de Ajustamento de Conduta (TAC) com o Ministério Público do Distrito Federal e Territórios (MPDFT) e aceitou pagar R\$ 500 mil a título de indenização por danos morais coletivos¹⁶⁰. Não há notícia, no entanto, que tal fato tenha abalado a confiança do consumidor nacional nessa varejista¹⁶¹.

¹⁵⁸MOREIRA, Braitner. Netshoes deverá procurar 2 milhões de clientes afetados por vazamento, diz MP. **G1-DF**. Publicado em 26 jan. 2018. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/mp-pede-que-netshoes-tome-providencia-apos-vazamento-de-2-milhoes-de-contas.ghtml>. Acesso em: 20 ago. 2023.

¹⁵⁹ Entre os emails de órgãos públicos cadastrados havia contas, segundo o MPDFT, do Tribunal de Contas da União (TCU), da Câmara dos Deputados, do Tribunal de Justiça do Distrito Federal e Territórios (TJDFT), da Polícia Federal, do Superior Tribunal de Justiça (STJ), do Supremo Tribunal Federal (STF), do Ministério da Justiça e da Advocacia-Geral da União e Presidência da República.

¹⁶⁰ DANTAS, Thaila. Netshoes terá de pagar R\$ 500 mil por vazamento de dados de milhões de clientes. **JusBrasil**. Disponível em: <https://www.jusbrasil.com.br/noticias/netshoes-tera-de-pagar-r-500-mil-por-vazamento-de-dados-de-milhoes-de-clientes/685006882>. Acesso em: 20 ago. 2023.

¹⁶¹ De acordo com a plataforma “ReclameAQUI”, a empresa Netshoes conta, no mês de agosto de 2023, com avaliação de confiabilidade geral de “8,3”: nível considerado “ótimo”, o maior da plataforma – e superior a outras empresas do setor, como a “Centauro” (índice 7,4, considerado “bom”) e a “Nike” (índice 7,5, considerado “bom”). RECLAME AQUI. **Netshoes**. Disponível em: <https://www.reclameaqui.com.br/empresa/netshoes/>. Acesso em: 20 ago. 2023. Consoante informa o site – largamente conhecido em solo nacional como indicador da qualidade do serviço prestado por empresas que atuam em âmbito digital – baseado nas avaliações dos consumidores, o Reclame Aqui analisa alguns critérios para a formulação da reputação. São eles: Índice de Resposta (IR) - Porcentagem de reclamações respondidas, sendo que apenas a primeira resposta é considerada; Média das Avaliações (Nota do Consumidor) (MA) - Leva em consideração apenas reclamações finalizadas e avaliadas. Corresponde à média aritmética das notas (variando de 0 a 10) concedidas pelos reclamantes para avaliar o atendimento recebido. Índice de Solução (IS) - Leva em consideração apenas reclamações finalizadas e avaliadas. Corresponde à porcentagem de reclamações onde os consumidores, ao finalizar, consideraram que o problema que originou a reclamação foi resolvido; Índice de Novos Negócios (Voltaria a fazer negócios?) (IN) - Leva em consideração apenas reclamações finalizadas e avaliadas. Corresponde à porcentagem de reclamações onde os consumidores, ao finalizar, informaram que, sim, voltariam a fazer negócios com a empresa. Para cálculo da Avaliação do Reclame AQUI (AR) é feita uma média ponderada baseada nesses critérios. Todos eles possuem valores que variam de 0 a 100, com exceção da Média (varia de 0 a 10), assim o valor da média das avaliações é multiplicado por 10, para estar na mesma escala das demais. Os critérios possuem pesos distintos, conforme segue: Índice de Resposta - Peso 2; Média das Avaliações (Nota do Consumidor) - Peso 3; Índice de Solução - Peso 3; Índice de Novos Negócios (Voltaria a fazer negócios?) - Peso 2. Assim a fórmula para obtenção da Avaliação do Reclame AQUI é a seguinte: $AR = ((IR * 2) + (MA * 10 * 3) + (IS * 3) + (IN * 2)) / 100$. Para $8 \leq AR \leq 10$, ÓTIMO; para $7 \leq AR < 8$

Após tratar das “vidas” e “instituições”, Carissa se dedica ao que nomeia de “sociedades envenenadas”. Conforme a autora, há quatro maneiras principais de se envenenar as sociedades com a má administração de dados pessoais, que pode: “comprometer a segurança nacional, podem ser usados para corromper a democracia, podem ameaçar as sociedades liberais ao promover uma cultura de exposição e vigilantismo, e podem colocar em risco a segurança dos indivíduos”. (VÉLIZ, 2021, p. 137).

Quanto ao primeiro aspecto concernente às “sociedades envenenadas”, o que busca salientar a autora – algo que continuará realizando em sua obra, ao longo dos outros enfoques – é a necessidade urgente de uma regulamentação e segurança cibernética eficaz, uma vez que a vulnerabilidade aos ataques desse tipo e ao uso indevido de dados é uma preocupação crescente em todo o mundo. A fim de justificar sua posição, apresenta exemplos que demonstram, a um, como a má administração de dados pessoais pode representar uma ameaça significativa à segurança nacional – o que à frente fará em relação à privacidade dos cidadãos e à integridade das instituições democráticas.

Um exemplo marcante é o caso da *Equifax*, uma das maiores corretoras de dados e agências de crédito do mundo, que sofreu uma violação de segurança cibernética em setembro de 2017. Nesse incidente, criminosos acessaram-se os dados pessoais de aproximadamente 147 milhões de cidadãos estadunidenses, incluindo informações sensíveis como nomes, números de previdência social, datas de nascimento e endereços (*Idem*). Este episódio foi considerado uma das maiores violações de dados da história, e gerou à empresa uma multa superior a R\$ 2 bilhões de reais¹⁶². Além disso, possui contornos ainda mais preocupantes: em fevereiro de

7.9, BOM; para 6 =< AR <= 6.9, REGULAR; para 5 =< AR <= 5.9, RUIM; para AR < 5, NÃO RECOMENDADA. Essa fórmula só é aplicada se a empresa passar por 2 avaliações prévias: Possuir índice de resposta superior à 50%. Se possuir um índice de resposta inferior a 50%, ela automaticamente é categorizada como NÃO RECOMENDADA. Isso é feito para garantir que empresas que não respondem a seus consumidores não sejam beneficiadas, pois todos os parâmetros analisados são obtidos a partir do atendimento realizado pelas empresas; Possuir um número de avaliações igual ou superior a 10. Se possuir menos, a empresa ficará com reputação SEM ÍNDICE. RECLAME AQUI. **Como funcionam os critérios para avaliação das empresas?** Disponível em: <https://www.reclameaqui.com.br/como-funciona/reputacao/>. Acesso em: 20 ago.2023.

¹⁶² No Brasil, a questão foi assim noticiada: FOLHA DE S. PAULO. **Equifax pagará até 700 milhões em acordo sobre violação de dados nos EUA.** Disponível em: <https://www1.folha.uol.com.br/mercado/2019/07/equifax-pagara-ate-us-700-milhoes-em-acordo-sobre-violacao-de-dados-nos->

2020, o Departamento de Justiça dos Estados Unidos acusou quatro militares chineses de nove acusações relacionadas com a violação – algo negado, até agora, pela própria China¹⁶³.

A questão crucial indicada por Carissa é por que os militares chineses teriam interesse em tais informações pessoais. Uma possibilidade é que eles buscavam identificar alvos em potencial para recrutamento como espiões. O acesso a informações detalhadas sobre indivíduos aumentaria as chances de sucesso em tais recrutamentos, pois possibilitaria o uso de chantagem ou persuasão com base em informações confidenciais (*Ibidem*, p. 138).

Além disso, países estrangeiros podem desejar esses dados para treinar algoritmos, uma vez que algoritmos treinados com base em dados chineses podem não ser eficazes em prever o comportamento de cidadãos ocidentais. Outra razão pode ser o uso desses dados para criar campanhas de desinformação direcionadas, como o caso da *Cambridge Analytica*. Além disso, os dados pessoais podem ser uma mercadoria negociável entre governos, com países como Rússia e Coreia do Norte também interessados em obter informações sobre americanos.

Outro aspecto tido pela autora como preocupante é o acesso a dados de localização, que pode ser comprado legalmente de corretores de dados¹⁶⁴. Isso foi evidenciado quando o *New York Times* recebeu dados de localização de um corretor de dados que estava preocupado com o potencial abuso dessas informações. Os dados incluíam informações sobre 12 milhões de telefones nos EUA e revelaram informações delicadas, como visitas a clínicas de saúde mental, locais LGBTQIAPN+, igrejas e mesquitas (*Ibidem*, p. 139-140). Esses dados podem ser usados para chantagear, seguir e até mesmo ameaçar indivíduos.

Essa facilidade de acesso a dados sensíveis pode tornar até mesmo os oficiais de segurança nacional e militares vulneráveis a ameaças. No caso do aplicativo de

eua.shtml#:~:text=A%20Equifax%20foi%20multada%20em,os%20armazenado%20nos%20Estados%20Unidos. Acesso em: 21 ago. 2023.

¹⁶³ O GLOBO. **Estados Unidos acusam quatro militares chineses por roubo de dados de quase 150 milhões de pessoas**. Publicado em 10 fev. 2020 Disponível em: <https://oglobo.globo.com/mundo/estados-unidos-acusam-quatro-militares-chineses-por-roubo-de-dados-de-quase-150-milhoes-de-pessoas-24240625>. Acesso em: 21 ago. 2023.

¹⁶⁴ Conforme documento confeccionado pela própria *Apple*, “Um corretor coleta dados sobre 700 milhões de consumidores em todo o mundo, criando perfis de consumidor com até cinco mil características”. Disponível em: https://www.apple.com/br/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf. Acesso em: 21 ago. 2023.

encontros *Grindr*, dados pessoais, incluindo conversas privadas e informações sobre o HIV, foram compartilhados com terceiros sem o devido consentimento. Isso levantou preocupações com a possibilidade de chantagem e revelações comprometedoras (*Ibidem*, p. 140-141).

Outro caso ilustrativo envolveu o uso público de aplicativos de rastreamento de corridas, como o *Strava*, por militares e funcionários do governo dos EUA. Ao compartilharem rotas de corrida, inadvertidamente revelaram informações sensíveis, incluindo a localização de bases secretas do exército. Essa divulgação acidental de informações pode ter graves implicações de segurança nacional, uma vez que potências estrangeiras podem usar esses dados para identificar alvos e atividades militares (*Ibidem*, p. 141-142).

Conforme argumenta Carissa Véliz, a má administração de dados pessoais representa, portanto, uma ameaça significativa à segurança nacional – e, com isso, à própria integridade das instituições democráticas. Razão pela qual se dedica a pensar as próprias ameaças à democracia decorrentes dessa toxicidade dos dados pessoais.

A questão das ameaças à democracia – que ganha, em razão dos objetivos do presente trabalho, destacada relevância – é evidenciada pelo escândalo outrora mencionado, envolvendo a empresa *Cambridge Analytica*. Este caso ilustra como as violações de privacidade podem desencadear a manipulação dos processos democráticos. A violação da privacidade possibilitou a construção de perfis detalhados que foram utilizados para direcionar campanhas políticas específicas às tendências psicológicas individuais das pessoas¹⁶⁵. Christopher Wylie, o denunciante da *Cambridge Analytica*, argumenta que o *Brexit*¹⁶⁶ não teria sido aprovado no referendo sem a interferência da empresa. Essa intervenção prejudicou não apenas os cidadãos dos países afetados, mas também aqueles de outras nações, uma vez que todos são

¹⁶⁵ Para uma compreensão completa sobre os fatos que geraram o chamado “escândalo de dados do Facebook–*Cambridge Analytica*”, em que as informações de mais de 87 milhões de pessoas foram utilizadas, sem os seus consentimentos, pela empresa americana *Cambridge Analytica* – que trabalhou para a campanha eleitoral do presidente estadunidense Donald Trump, no ano de 2016 – para fazer propaganda política, e que culminou com a eleição de Trump para a presidência dos Estados Unidos, naquele mesmo ano, ver KAISER (2019). Na mídia, pode-se consultar o seguinte: G1. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades.** Publicado em 20 mar. 2018. 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: 21 ago. 2023.

¹⁶⁶ A saída do Reino Unido da União Europeia foi apelidada de *Brexit*, originada na língua inglesa, resultante da junção das palavras *British* e *exit*.

influenciados pela política global. Isso destaca o alcance dos danos causados pelos abusos de dados.

Chris Sumner, diretor de pesquisa e co-fundador da *Online Privacy Foundation*, conduziu um estudo sobre anúncios políticos ditos “obscuros”. Esses anúncios são visíveis apenas para o anunciante e o público-alvo, e podem ser direcionados com base em dados de localização, comportamento e características psicográficas das pessoas. Sumner realizou um experimento direcionado a 2.412 pessoas no *Facebook*, dividindo-as em dois grupos com tendências autoritárias altas e baixas. Em seguida, criou quatro campanhas publicitárias diferentes. Os resultados revelaram que os anúncios personalizados eram mais eficazes em seus grupos-alvo específicos. Por exemplo, o anúncio favorável à vigilância, direcionado a personalidades altamente autoritárias, obteve vinte vezes mais interações do que o grupo com tendências autoritárias baixas. No entanto, não ficou claro como essas métricas se traduzem em votos (*Ibidem*, p. 143).

Alguns céticos argumentam que o microdirecionamento tem efeitos limitados nas eleições devido à fraca correlação entre traços pessoais e preferências políticas. Além disso, o poder preditivo dos likes no *Facebook* pode ser volátil ao longo do tempo e ser influenciado por eventos políticos importantes. As campanhas políticas também enfrentam a competição de outras usando as mesmas táticas, o que pode anular alguns efeitos. (*Ibidem*, p. 144).

No entanto, a preocupação persiste de que o microdirecionamento possa ter um impacto significativo, mesmo que limitado. Pesquisas sugerem que quando um eleitor é exposto a conteúdo político que se alinha com suas opiniões em questões específicas, é mais provável que vote de acordo com essas preferências ou que se abstenha de votar. (*Ibidem*, p. 145).

Além disso, mesmo pequenos efeitos podem ser significativos quando se trata de eleições, especialmente em disputas acirradas. O exemplo de um estudo realizado pelo *Facebook* durante as eleições para o Congresso dos Estados Unidos em 2010 demonstra como pequenos incentivos podem influenciar os eleitores e potencialmente mudar o resultado de uma eleição.

A ameaça da interferência eleitoral e o papel das redes sociais, como o *Facebook*, entre outros, nas eleições são preocupações importantes. As redes sociais

têm um alcance significativo sobre os eleitores, e sua capacidade de moldar o discurso político e influenciar o comportamento dos eleitores deve ser considerada seriamente. A manipulação das eleições prejudica a confiança no processo democrático e pode minar a legitimidade do governo eleito.

A fragmentação da esfera pública devido ao direcionamento personalizado de anúncios políticos é outro problema crítico. Quando as pessoas são expostas a informações divergentes e potencialmente contraditórias, a capacidade de conduzir debates políticos saudáveis é comprometida. Isso contrasta com o ambiente em que todos veem os mesmos anúncios, permitindo discussões informadas e escrutínio público¹⁶⁷.

Portanto, é essencial lidar com os desafios associados à manipulação de dados, à privacidade e à influência das redes sociais nas eleições para manter a integridade dos processos democráticos e proteger a esfera pública. Medidas regulatórias podem ser necessárias para garantir eleições justas e transparentes, evitando que empresas privadas influenciem desproporcionalmente o resultado das eleições e minem a democracia.

Retomando, nesse contexto, aspectos alhures mencionados acerca da importância da democracia e sua interação com a proteção de dados pessoais, vê-se que a crescente digitalização da vida, quando mal regulada, representa uma ameaça direta à democracia, na medida em que pode intensificar desigualdades e concentrar poder nas mãos de um pequeno número de corporações e governos que controlam os fluxos de dados globais. O fenômeno do "colonialismo de dados" exemplifica esse risco. No cenário contemporâneo, o controle sobre os dados equivale ao controle sobre o comportamento e a tomada de decisões das populações. Grandes empresas de tecnologia, com acesso ilimitado a dados pessoais, têm a capacidade de influenciar processos políticos, moldar o debate público e até mesmo manipular eleições – como reiteradamente demonstrado pelo caso da *Cambridge Analytica*. Essa concentração de poder compromete a soberania dos Estados e enfraquece a capacidade de suas instituições democráticas de agir em prol do bem comum.

¹⁶⁷ Sobre o assunto, a escrita de Carissa Véliz é contundente e pertinente, ao indicar que: “Um dos mais importantes pilares de uma democracia saudável é a realização de eleições justas. Não só isso, as pessoas têm de se sentir confiantes sobre a justiça do processo eleitoral. Se a maioria dos cidadãos suspeitar de interferência eleitoral, a legitimidade do governo pode ser seriamente comprometida”. (VÉLIZ, 2021, p. 148).

O problema se agrava quando observamos que a legislação de muitos países do Sul Global, como o Brasil, está em um processo de adaptação às rápidas mudanças tecnológicas, enquanto as grandes corporações de dados, sediadas majoritariamente em países centrais, operam com poucos limites. O Brasil, com a promulgação da Lei Geral de Proteção de Dados (LGPD), deu um passo importante na direção de proteger os direitos dos seus cidadãos no ambiente digital. No entanto, o desafio maior reside na implementação e fiscalização eficazes da lei, especialmente no que se refere à transferência internacional de dados. A ausência de uma regulamentação forte sobre esse tema permite que dados brasileiros sejam manipulados por entidades estrangeiras, que não têm qualquer vínculo ou responsabilidade direta com a população afetada.

A transferência internacional de dados sem a devida proteção é uma ameaça significativa à transparência, à responsabilidade democrática e à própria ideia de soberania nacional. Quando dados pessoais de brasileiros são enviados para países com legislações mais flexíveis, os cidadãos perdem o controle sobre suas informações e, conseqüentemente, sobre sua autonomia. Esse cenário pode facilitar o surgimento de novos mecanismos de controle social e manipulação política, nos quais interesses externos têm maior poder de influência sobre as decisões nacionais do que o próprio governo democraticamente eleito. Em um Estado Democrático de Direito, é essencial que a proteção dos dados pessoais seja vista como parte integrante dos direitos fundamentais, garantindo que todos os cidadãos possam exercer sua liberdade política sem interferências indevidas ou vigilância não consentida.

Portanto, as ameaças à democracia no contexto da proteção de dados pessoais exigem uma resposta robusta e coordenada por parte dos Estados, especialmente no que tange à cooperação internacional para garantir que as transferências de dados sejam realizadas com pleno respeito aos direitos dos indivíduos. O papel da Autoridade Nacional de Proteção de Dados (ANPD) no Brasil é crucial para assegurar que o país esteja alinhado às melhores práticas internacionais, sem abrir mão de sua soberania informacional. A adoção de "decisões de adequação", que garantem que os países destinatários dos dados brasileiros sigam padrões equivalentes aos da LGPD – e de outras possíveis elaborações normativas que impactem na tutela dos dados pessoais em âmbito nacional – é uma

medida fundamental para prevenir abusos e proteger a integridade do processo democrático.

O terceiro aspecto salientado pela autora se refere às ameaças às sociedades liberais¹⁶⁸, ao se promover, a partir da captura e tratamento de dados pessoais, uma cultura de exposição e vigilantismo. Conforme afirma, o cerne dessas sociedades reside no princípio fundamental que concede aos indivíduos a prerrogativa de conduzir suas vidas conforme seus próprios desejos (*Ibidem*, p. 153). Esta premissa consagra uma presunção intrínseca em prol da liberdade, refletida na célebre aforação de John Stuart Mill, que estabelece que "o ônus da prova recai sobre aqueles que buscam impor restrições ou proibições." (*Idem*). Como corolário desse princípio, é imperativo estabelecer normas destinadas a evitar danos individuais, garantir que os cidadãos estejam isentos de interferências indevidas e, simultaneamente, promover uma vida em sociedade na qual todos possam participar.

A salvaguarda da privacidade desempenha um papel crucial na construção de um espaço privado robusto, proporcionando uma zona de resguardo na sociedade

¹⁶⁸ A defesa da autora se volta, nesse ponto, à filosofia pensada pelo chamado "liberalismo político". Consoante definição de Nicola Abbagnano, o Liberalismo é a "doutrina que tomou para si a defesa e a realização da liberdade no campo político". (ABBAGNANO, 2007, p. 604). No entanto, conforme o próprio Abbagnano, o Liberalismo, na medida que vivido e pensado por diferentes atores e instituições ao longo da história, tomou contornos que vão muito além de uma definição ingênua e singela de *doutrina defensora da liberdade*. Com efeito, a par da defesa da Democracia política e dos Direitos Humanos, não raras vezes acompanha o pensamento liberal a defesa do capitalismo de livre mercado. Tal complexidade deve ser pensada de forma mais profunda e responsável, mormente a partir de países periféricos – o que se propõe em tópico a ser abordado ainda nesse capítulo. Sobre o assunto, a lição de Abbagnano: "Portanto, um grande número de correntes políticas díspares e por vezes opostas puderam falar em nome do L. (DE RUGGIERO, Storia dei L. europeo, 1925): partidos que negaram o valor do Estado (como o radicalismo inglês do século passado), partidos que exaltaram o valor do Estado (como a chamada "direita histórica" da Itália após o "*resorgimento*"), partidos que recusaram qualquer ingerência do Estado em assuntos econômicos (como fazem ainda hoje alguns partidos liberais europeus), partidos que defendem a intervenção do Estado na iniciativa e na direção dos negócios econômicos, partidos que consideraram a liberdade como condição para a prática de qualquer atividade humana e partidos que a relegaram para o empíreo dos "valores" puros. Esses contrastes são a manifestação evidente do caráter compósito da doutrina liberal, caráter este que decorre do modo aproximativo e confuso como foi tratada a noção que deveria ser fundamental para o L. a de liberdade. O recurso casual ou sub-reptício a um ou outro dos conceitos de liberdade elaborados na história do pensamento filosófico tornou a ideia liberal em política confusa e oscilante, conduzindo-a por vezes à defesa e à aceitação da não-liberdade (v. LIBERDADE)". (ABAGGNANO, 2007, p. 605). Importante salientar, por fim, que o "liberalismo" referenciado por Carissa Véliz corresponde, a partir do que reflete em sua obra, à perspectiva política e teórica (sem quaisquer incursões, portanto, nos efeitos desse pensamento nos países periféricos) que textualmente indica logo ao introduzir o assunto, ao afirmar que "o princípio básico das sociedades liberais é que os indivíduos devem ter a liberdade de viver suas vidas como lhes aprouver. (...) Devem ser estabelecidas regras para evitar danos às pessoas, para assegurar que os cidadãos estejam livres de interferências desnecessárias e para estabelecer uma vida comum na qual todos possam participar". (VÉLIZ, 2021, p. 153). Não confundir, portanto, com o "neoliberalismo", tratado – e criticado – no tópico seguinte.

na qual os indivíduos possam desfrutar de momentos e lugares livres dos escrutínios, julgamentos, inquirições e intromissões alheias¹⁶⁹. As normas de privacidade exercem uma função inestimável, ao proporcionar o espaço necessário para o desenvolvimento pessoal. É crucial salientar que um nível saudável de reserva e confidencialidade é essencial para o funcionamento harmonioso da sociedade civilizada. Imaginar um cenário em que todos pudessem ler os pensamentos uns dos outros reduziria o espaço privado à inexistência, poluindo, assim, a esfera pública com infundáveis e evitáveis conflitos. Portanto, o liberalismo não se limita à mera restrição do governo na esfera privada dos cidadãos; para prosperar, deve ser inculcado em uma cultura de moderação, na qual os indivíduos comuns se esforcem para permitir que outros vivam suas vidas livremente.

As redes sociais contemporâneas, por sua vez, incentivam incansavelmente o "compartilhamento" de informações pessoais online. O modelo de negócios da Meta, por exemplo, depende da revelação constante de aspectos pessoais pelos usuários. Quando esses usuários compartilham menos informações pessoais, as plataformas de redes sociais sentem a necessidade de ajustar seus algoritmos para incentivar um maior compartilhamento. A mensagem implícita é clara: compartilhe tudo o que puder. Revela-nos sua identidade, emoções, detalhes sobre sua família e amigos, bem como suas opiniões sobre outras pessoas. Anuncie ao mundo o que pensa. O imperativo é saber, ouvir e, sobretudo, dar voz ao que tem a dizer. (*Ibidem*, p. 154).

Entretanto, as redes sociais fomentam uma cultura que desencoraja a contenção. Quanto mais as pessoas compartilham, mais dados podem ser coletados e utilizados para fins comerciais. Quanto mais comentários são feitos sobre o que outros compartilham, mais cliques, anúncios, receitas e poder são gerados. Superficialmente, essa parece uma situação em que todos saem ganhando: os indivíduos têm a oportunidade de se expressar incessantemente, enquanto as empresas de tecnologia sustentam seus negócios. No entanto, é crucial reconhecer

¹⁶⁹ Quanto a compreensão do termo "privacidade", remete-se às reflexões realizadas no início do capítulo. No presente momento, verifica-se a ênfase da autora na compreensão da privacidade enquanto direito individual estático e subjetivo, ou seja, mais voltado a um "direito a ser deixado só", ou, ainda, sobre a "proteção contra interferências de terceiros" – o que não significa que os dados pessoais cumpram um papel diminuído nesse âmbito. Ao revés, o que se verificará é que ocupam o centro de um sistema de vigilância que busca monitorar a sociedade: fenômeno conhecido por *surveillance*, nos termos empregados por Zygmunt Bauman.

que grande parte do que é compartilhado online não beneficia os próprios usuários. Os dados pessoais dos indivíduos são explorados de maneiras que não promovem seus interesses, e aquilo que compartilham os expõe a outros usuários que, em alguns casos, estão dispostos a explorar, chantagear ou humilhar.

O liberalismo, em seu âmago, preconiza que nada deve ser submetido ao escrutínio público além do necessário para proteger os indivíduos e promover uma vida coletiva saudável. Em contrapartida, uma cultura de exposição demanda que tudo seja compartilhado e sujeito à avaliação pública. As gigantes da tecnologia vendem a ideia de que a transparência é uma virtude universal, alegando que "quem não deve, não teme." No entanto, os exibicionistas que expõem outras pessoas não agem de maneira virtuosa. Na economia digital, todos são pressionados a revelar mais do que seria necessário para fins de amizade, comunicação eficaz e debates públicos construtivos, tudo em nome da criação de mais dados. (*Ibidem*, p. 156).

O compartilhamento excessivo beneficia principalmente as grandes empresas de tecnologia, não os próprios usuários. Essa pressão constante para compartilhar conduz a expressões de agressão e intolerância, e alimenta o "vigilantismo". Cada dado pessoal é coletado, monetizado pelas empresas, examinado e, por vezes, explorado em atos públicos de humilhação virtual por parte dos internautas. A incessante disputa sobre os detalhes do que as pessoas dizem e fazem na internet desvia nossa atenção de conversas mais substanciais, aquelas que abordam questões de justiça, economia, ecologia e o bem comum. Enquanto nos afundamos em intermináveis discussões virtuais, alimentando conflitos e revelando fraquezas humanas alheias às quais também somos vulneráveis, nossas democracias enfrentam um perigo iminente (*Ibidem*, p. 156).

Em muitos aspectos, as culturas de exposição assemelham-se à brutalidade inerente às relações sociais infantis. As crianças são notórias tanto por não compreenderem os limites do que é apropriado dizer quanto por seu potencial crueldade, especialmente quando atuam em grupo. À medida que a internet amadurece, é possível que nos afastemos de uma cultura de compartilhamento excessivo e de intimidação, buscando formas mais maduras de interação e relacionamento interpessoal.

No entanto, apesar de Carissa Véliz indicar que entre as ameaças mais graves ao liberalismo político encontravam-se as atividades ligadas ao que chamou de “vigilantismo”, o foco principal de seu escrito, consoante se observa, é o que denomina de “cultura de exposição”. Uma análise mais aprofundada da questão, no entanto, indica que tal cultura, em verdade, é parte integrante de um fenômeno amplo e complexo, mais próximo do que denomina, justamente, de “vigilantismo” – e cujo termo mais apropriado ainda responde, apesar de indesejados estrangeirismos, pelo anglicismo *surveillance*.

Surveillance é um termo em inglês comumente traduzido como vigilância. Entretanto, a mesma locução pode ser utilizada para explicar o vocábulo *vigilance*. A forma que o ato de se observar determinada pessoa ou fenômeno de maneira atenta, e às vezes oculta, assumiu na atualidade, auxiliado por mecanismos tecnológicos que permite a captura e a guarda de centenas de milhares de informações, aponta para a insuficiência da utilização do termo vigilância em sua acepção original, dando lugar a um novo conceito, mais amplo e dinâmico, explicitado através de mencionado estrangeirismo¹⁷⁰.

Nesse contexto, *surveillance* não admite tradução como mera vigilância, ou seja, um evento específico e dirigido contra determinados sujeitos, porquanto tributária de uma dilatação desse conceito, permitido pelas modernas táticas de observação, categorização e esquadrinhação da sociedade, angariando a ele novas e complexas perspectivas¹⁷¹, razão pela qual, mais do que se optar pela utilização do vocábulo *surveillance* em vez do “vigilantismo” empregado por Carissa¹⁷², deve-se também colocá-lo como característica inerente do mundo ocidental contemporâneo.

¹⁷⁰ Nesse sentido a lição Elias Jacob de Menezes Neto, ao afirmar que “o uso comum da expressão *surveillance* fez com que ela permanecesse sendo traduzida para o português como ‘vigilância’. No entanto, como será visto, a *surveillance* deixou de ser mera vigilância, ou seja, um evento específico e dirigido contra determinados sujeitos, passando a constituir uma das características inevitáveis das sociedades contemporâneas”. (JACOB NETO, 2014. p. 532).

¹⁷¹ . Quanto a esse aspecto, importante a contribuição de José Luís Bolzan de Moraes e Elias Jacob de Menezes Neto, quando afirmam: entende-se, portanto, que as novas infraestruturas da tecnologia da informação, ao permitirem o processamento em tempo real e o armazenamento ilimitado de dados, não apenas “qualificam” a vigilância, mas introduzem mudanças qualitativas que permitem um “salto” em direção ao conceito de *surveillance*. (BOLZAN DE MORAIS; MENEZES NETO, 2013, p. 421)

¹⁷² Não há qualquer reparo a ser realizado na tradução da obra original ao português, na medida que Carissa Véliz utiliza, efetivamente, o termo “*vigilantism*”. A opção da autora por referido termo é obscura; com efeito, ao se pesquisar, no texto original, pelo termo “*surveillance*”, verifica-se que

O controle social por meio de técnicas de vigilância foi tradicionalmente pensado pelo filósofo inglês Jeremy Bentham (2008), mediante a proposição da noção de Panóptico. O Panóptico traduz, enquanto arquétipo prisional, uma forma de se instaurar uma vigilância onipresente capaz de exercer o controle social de forma efetiva e sem violência física sobre os indivíduos. Isto se daria por meio da construção de uma estrutura física circular contendo várias celas ao redor de um pátio com uma torre ao centro, permitindo que todo o espaço fosse inteiramente observável – sem, contudo, que o observador, que, em tese, habitava o alto da torre, fosse visto. Era na

aparece, durante a obra, mais de 190 (cento e noventa) vezes. No entanto, no capítulo dedicado à toxicidade dos dados pessoais, é empregado apenas 8 (oito) vezes, todas em um mesmo contexto: o de relatar o projeto de pesquisa liderado por Chris Sumner, diretor de pesquisa e cofundador da *Online Privacy Foundation*, uma organização sem fins lucrativos, sobre “anúncios obscuros”. A autora não o utiliza, portanto, com a finalidade de expor seu próprio ponto de vista, mas de relatar um ato praticado por terceiro. Com essa finalidade, o termo “*surveillance*” foi traduzido ao português como “vigilância”. Confira-se a redação original do excerto: “*Sumner and Shearing then created advertisements that either supported or opposed state mass surveillance. The team created four different ad campaigns. The pro-surveillance ad designed for people high in authoritarianism showed a picture of bombed buildings and read: ‘Terrorists – Don’t let them hide online. Say yes to mass surveillance.’ The version created for people with low authoritarian tendencies read: ‘Crime doesn’t stop where the Internet starts. Say yes to surveillance.’ The anti-surveillance ad tailored to people with high levels of authoritarianism carried an image of the D-Day landings and read: ‘They fought for your freedom. Don’t give it away! Say no to mass surveillance.’ The version tailored to people with low levels of authoritarianism showed a photograph of Anne Frank and read: ‘Do you really have nothing to fear if you have nothing to hide? Say no to state surveillance.’ Tailored ads were more effective with their intended target groups. The ad that supported surveillance and targeted high authoritarian personalities, for instance, had twenty times as many ‘likes’ and shares from the high-authoritarianism group than from the low one. People classified as highly authoritarian were significantly more likely to share an ad designed for them, and people classified as having low levels of authoritarian tendencies thought that ads designed for them were more persuasive than those ads that were designed for their opposites. What is not clear, however, is how these metrics (likelihood of sharing a post, and finding an ad persuasive) translate into votes”.* (VÉLIZ, 2020, p. 48-49). A tradução ao português foi assim realizada: “Sumner e Shearing, então, criaram propagandas que apoiavam ou se opunham à vigilância em massa do estado. A equipe criou quatro campanhas publicitárias diferentes. O anúncio pró-vigilância projetado para pessoas com alto grau de autoritarismo mostrava uma imagem de edifícios bombardeados e dizia: “terroristas — não os deixem se esconder online. Diga sim à vigilância em massa”. A versão criada para pessoas com tendências pouco autoritárias dizia: “o crime não para onde a internet começa. Diga sim à vigilância”. Do outro lado, o anúncio antivigilância feito para pessoas com altos níveis de autoritarismo trazia uma imagem das aterrissagens do Dia D e dizia: “eles lutaram por sua liberdade. Não abra mão dela! Diga não à vigilância em massa”. A versão adaptada para pessoas com baixos níveis de autoritarismo mostrou uma fotografia de Anne Frank e dizia: “você realmente não tem nada a temer se não tem nada a esconder? Diga não à vigilância estatal”. Os anúncios sob medida eram mais eficazes com seus grupos-alvo pretendidos. O anúncio que apoiava a vigilância e visava personalidades altamente autoritárias, por exemplo, tinha vinte vezes mais *likes* e compartilhamentos do grupo com alto nível de autoritarismo do que o grupo com menor nível. As pessoas classificadas como altamente autoritárias tinham uma probabilidade significativamente maior de compartilhar um anúncio projetado para elas, e as pessoas classificadas como tendo baixos níveis de tendências autoritárias pensavam que os anúncios projetados para elas eram mais persuasivos do que aqueles que foram projetados para seus opostos. O que não ficou claro, entretanto, é como essas métricas (probabilidade de compartilhar uma publicação, e achar um anúncio persuasivo) se traduzem em votos”. (VÉLIZ, 2021, p. 143-144).

suposta presença constante do observador, portanto, somada à sua invisibilidade, que residia a inventividade da estrutura arquetípica.

O filósofo francês Michel Foucault percebeu que o mecanismo arquitetural de Bentham oferecia uma chave para se compreender a ascensão das sociedades modernas e autodisciplinadas. Assim o fez em sua clássica obra *Surveiller et Punir: naissance de la prison* (2008), apontando-o como a suma encarnação de uma moderna instituição disciplinar.

Para Foucault o efeito mais importante do Panóptico era justamente aquele detectado por Bentham: induzir no detento um estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder¹⁷³. Nesse sentido, utilizou o projeto de Bentham como arquimetáfora do poder moderno. Da maneira como afirmada pelo filósofo francês: “é ao mesmo tempo excessivo e muito pouco que o prisioneiro seja observado sem cessar por um vigia: muito pouco, pois o essencial é que ele se saiba vigiado; excessivo, porque ele não tem necessidade de sê-lo efetivamente”¹⁷⁴. Isso significa que a visibilidade se torna uma armadilha – mas uma armadilha que nós mesmos, na modernidade, ajudamos, subjetivamente, a construir¹⁷⁵.

Anos mais tarde, Zygmunt Bauman também faria uso, em diferentes obras, do exemplo do Panóptico, a fim de demonstrar como a vigilância era pensada na época da modernidade que caracteriza como “pesada” – e que se diferencia, do presente estágio da modernidade, a quem chama de “fluida”, quanto às técnicas de controle¹⁷⁶.

¹⁷³ Nesse sentido, escreve Foucault: “Fazer com que a vigilância seja permanente em seus efeitos, mesmo se é descontínua em sua ação; que a perfeição do poder tenda a tornar inútil a atualidade de seu exercício; que esse aparelho arquitetural seja uma máquina de criar e sustentar uma relação de poder independente daquele que o exerce; enfim, que os detentos se encontrem presos numa situação de poder de que eles mesmos são os portadores. (*Ibidem*, p. 166-167).

¹⁷⁴ *Idem*.

¹⁷⁵ Novamente, Foucault: “Quem está submetido a um campo de visibilidade, e sabe disso, retoma por sua conta as limitações do poder; fá-las funcionar espontaneamente sobre si mesmo; inscreve em si a relação de poder na qual ele desempenha simultaneamente os dois papéis; torna-se o princípio de sua própria sujeição”. (*Ibidem*, p. 168).

¹⁷⁶ “Líquida” é o adjetivo utilizado por Zygmunt Bauman para caracterizar a atual disposição da sociedade, que também denomina de “sociedade da modernidade fluida”, em oposição à solidez vislumbrada na modernidade de outrora. (BAUMAN, 2001, p. 31). Buscando explicitar os principais motivos deste câmbio (solidez/liquidez), se utiliza das noções que os conceitos de “tempo” e “espaço” assumiram na sociedade contemporânea. Tais concepções possuem uma importância visceral na compreensão da realidade proposta por Bauman, tendo em vista que o adjetivo “líquido”, utilizado para caracterizar a modernidade, advém justamente de uma nova percepção destes fenômenos. Nesse sentido aduz que: “Os fluidos, por assim dizer, não fixam o espaço nem prendem o tempo. Enquanto os sólidos têm dimensões espaciais claras, mas neutralizam o impacto e, portanto, diminuem a

Nesse sentido, indica que, apesar de Bentham apresentá-lo como uma instituição particular, bem fechada em si mesma – uma espécie de utopia do encarceramento perfeito – o Panóptico deve ser compreendido, segundo Foucault, como um modelo generalizável de funcionamento, como uma maneira de definir as relações de poder com a vida quotidiana das pessoas. Na contemporaneidade, a contribuição dos dispositivos tecnológicos voltados à massiva observância social e à captação de dados fizeram com que o sociólogo polonês descrevesse os tempos atuais, em contraste com o anterior, marcado pelas técnicas tradicionais de vigilância, como uma era do pós-panóptico.

Com tal afirmação não busca afirmar, entretanto, que o modelo panóptico esteja, por completo, superado. Em verdade, suas modificações estruturais acabam por fortificá-lo, dando à vigilância um alcance jamais pensado na era da modernidade “sólida”¹⁷⁷. Apesar disso, não mais se apresenta como o modelo ideal de controle social, sendo relegado à manutenção de estruturas utilizadas, atualmente, quase que exclusivamente, para controlar aqueles que vivem à margem da sociedade¹⁷⁸.

significação do tempo (resistem efetivamente a seu fluxo ou o tornam irrelevante), os fluidos não se atêm muito a qualquer forma e estão constantemente prontos (e propensos) a mudá-la; assim, para eles, o que conta é o tempo, mais do que o espaço que lhes toca ocupar; espaço que, afinal, preenchem apenas “por um momento”. Em certo sentido, os sólidos suprimem o tempo; para os líquidos, ao contrário, o tempo é o que importa” (BAUMAN, 2001, p. 8). Para Bauman, a modernidade começa quando “espaço” e “tempo” se tornam conceitos separados, passíveis de teorizações distintas e mutuamente independentes da estratégia e da ação, em oposição a uma pré-modernidade que os concebia, a partir de sua experiência de vida, como inseparáveis (BAUMAN, 2001, p. 15). Um exemplo utilizado para demonstrar essa possibilidade de abordagem distinta destes conceitos diz respeito à “velocidade”, tendo em vista que esta pressupõe uma relação variável entre as dimensões tempo/espaço (BAUMAN, 2001, p. 16). Com efeito, o tempo representa, nas categorias propostas por Bauman, a parte dinâmica, ativa e “líquida” da sociedade, enquanto o espaço – pesado, inerte e impassível – tornava-se cada vez mais a representação do lado “sólido” da realidade, consistindo em um “obstáculo aos avanços do tempo”. Ocorre que, após um longo esforço para se acelerar mais e mais a velocidade do movimento, ao que tudo indica isto chegou ao seu “limite natural”. Com efeito, “quando a distância percorrida numa unidade de tempo passou a depender da tecnologia, de meios artificiais de transporte, todos os limites à velocidade do movimento, existentes ou herdados, poderiam, em princípio, ser transgredidos”. Na modernidade líquida, o tempo assume uma importância ainda maior que na modernidade sólida. Isso porque tal conceito foi combinado com uma crescente superação das barreiras físicas dos Estados, ao ponto de ocorrer um fenômeno determinado por Bauman como “anulação tecnológica das distâncias temporais/espaciais”.

¹⁷⁷ O que justifica a compreensão dessa vigilância, atualmente, como *surveillance*.

¹⁷⁸ Nesse sentido afirma Zygmunt Bauman: Tal como eu vejo, o panóptico está vivo e bem de saúde, na verdade, armado de músculos (eletronicamente reforçados, “ciborguizados”) tão poderosos que Bentham, ou mesmo Foucault, não conseguiria nem tentaria imaginá-lo; mas ele claramente deixou de ser o padrão ou a estratégia universal de dominação na qual esses dois autores acreditavam em suas respectivas épocas; nem continua a ser o padrão ou a estratégia mais comumente praticados. O panóptico foi tirado de seu lugar e confinado às partes “não administráveis” da sociedade, como prisões, campos de confinamento, clínicas psiquiátricas e outras “instituições totais”, no sentido criado por Goffman. (...) Em outras palavras, as práticas de tipo panóptico estão limitadas a locais destinados a

As razões para se apregoar, simultaneamente, o fortalecimento do arquétipo benthaniano, e sua superação enquanto modelo definidor do poder moderno, podem ser assim resumidas: a um, o Panóptico era um modelo de engajamento e confrontação mútuos entre os dois lados da relação de poder. De um lado, os internos, presos ao lugar e impedidos de qualquer movimento, confinados entre muros grossos, densos e bem-guardados, e fixados a suas camas, celas ou bancadas. Eles não podiam se mover porque estavam sob vigilância; tinham que se ater aos lugares indicados sempre porque não sabiam, e nem tinham como saber, onde estavam no momento seus vigias, livres para moverem-se à vontade. De outro, as estratégias dos administradores, mantendo sua própria volatilidade enquanto vigias da estrutura e rotinizando o fluxo do tempo de seus subordinados. Mas havia tensão entre as duas tarefas. A segunda tarefa punha limites à primeira — prendia os “rotinizadores” ao lugar dentro do qual os objetos da rotinização estavam confinados. Os “rotinizadores” não eram, portanto, verdadeira e inteiramente livres para moverem-se: a opção “ausente” estava fora de questão em termos práticos (BAUMAN, 2001, p. 16-17).

Nesse contexto, a ascensão das novas tecnologias, e seu emprego tanto no modelo panóptico de controle quanto nos novos modos de vigilância, promovem uma alteração fulcral na dinâmica supramencionada: dispensam, de todo, qualquer presença física dos “rotinizadores”, dos observadores.

O outro motivo diz respeito, justamente, à verificação de outras modalidades de vigilância adaptadas à realidade da modernidade fluida e possibilitadas pelos mecanismos tecnológicos de captação de dados pessoais, nas suas diferentes manifestações (v.g. imagem, áudio e informações textuais), das quais se destacam duas: o ban-óptico e o sinóptico.

O primeiro dos conceitos foi cunhado, originalmente, por Didier Bigo (2006)¹⁷⁹, em que as tecnologias de vigilância, em verdade, se preocupam muito mais em promover a exclusão dos elementos indesejados, no mais das vezes em nome da segurança, do que apostar no confinamento de indivíduos no modelo do panóptico; o

seres humanos categorizados na coluna dos débitos, declarados inúteis, plena e totalmente “excluídos” – e onde a incapacitação dos corpos, mais que seu aproveitamento para o trabalho útil, é o único propósito por trás da lógica do assentamento (BAUMAN, 2001, p. 58).

¹⁷⁹ A obra citada por Bauman se remete ao artigo escrito por Didier Bigo, intitulado *Globalized (in)security: the field of the ban-opticon*. In: SAKAI, Naoki; SOLOMON, Jon (orgs). **Traces 4: Translation, Biopolitics, Colonial Difference**, Hong Kong University Press, 2006.

ban-óptico, nesse sentido, deseja “manter à distância” certos indivíduos ou grupos sociais, eleitos como indesejáveis ou inimigos de determinada organização social.

Exemplo de dispositivos ban-ópticos podem ser relacionados às câmeras de TV que promovem a vigilância de comunidades fechadas e de shopping centers, a fim de barrar a entrada daqueles que não se coadunam aos padrões comportamentais esperados, como, por, por exemplo, os que não portam cartões de crédito ou telefones celulares, algo que os torna elementos não confiáveis da sociedade. Ao fim e ao cabo, a exclusão social é a razão de ser do ban-óptico¹⁸⁰.

O conceito de sinóptico é apresentado por Thomas Mathiesen, e se diferencia do panóptico justamente porque nesse, o termo se remete a uma ideia de *poucos vigiando muitos*, e, naquele, impera a realidade de *muitos vigiando poucos*. Para tanto, haveria como que uma transmissão dos deveres de vigilância aos próprios vigiados: uma vigilância sem vigilantes, no melhor estilo “panóptico: faça você mesmo”¹⁸¹.

Essa “privatização dos deveres modernizantes”¹⁸² (BAUMAN, 2001, p. 38.) é algo próprio da modernidade fluida. No campo da vigilância, ela se dá com a docilidade dos usuários de sistemas informatizados – o que representa, em verdade, parcela significativa da população mundial – seduzidos pelas funcionalidades e interações sociais promovidas por empresas atuantes na internet, a exemplo do Google e do Facebook. A cada acesso, os usuários fornecessem a matéria prima – nesse caso, os dados pessoais – que será utilizada pelos profissionais (mentes humanas ou artificiais, com larga vantagem para a segunda, na atualidade) a fim de delas retirarem “categorias-alvo”, ou seja, compradores potenciais dos bens de consumo disponíveis no mercado, que financiam, justamente, a atividade de captação dos dados¹⁸³.

¹⁸⁰ BAUMAN, 2014, p. 89.

¹⁸¹ *Ibidem*, p. 70.

¹⁸² A expressão significa a atribuição individual de responsabilidade pelas escolhas da vida em face de uma realidade mutável e incerta, tarefa que antes era ao menos dividida com a estrutura social ou estatal presentes na era da “modernidade pesada”.

¹⁸³ Sobre o sinóptico, afirma Bauman: “Se o sinóptico substitui o panóptico, não há necessidade de construir grandes muralhas e erigir torres de vigilância para manter os internos do lado de dentro, ao mesmo tempo contratando um número incalculável de supervisores para garantir que eles sigam a rotina prescrita; com o custo adicional de aplacar o ódio latente e a falta de disposição para cooperar que a rotina monótona em geral alimenta; assim como de precisar fazer um esforço contínuo para matar no nascedouro a ameaça de uma rebelião contra a indignidade da servidão. Agora, espera-se que os objetos de preocupação disciplinares dos gerentes se autodisciplinem e arquem com os custos materiais e psíquicos da produção da disciplina. Espera-se que eles mesmos ergam as muralhas e permaneçam lá dentro por vontade própria. A recompensa (ou a promessa) substitui a punição, e

Engana-se, entretanto, quem alia essa atividade de captação de dados a um aparato coercitivo, que obrigue os cidadãos, sob sanção, a entregarem seus dados às empresas atuantes no ambiente virtual. Ao revés. O que se verifica, na atual sociedade, é uma crescente *escopofilia* dos cidadãos. Esse termo tem, como significado, o *amor de ser visto*, e que possui sua gênese, em verdade, no sentimento de que a própria existência social do cidadão depende e está vinculada à sua existência no mundo virtual. Nesse sentido, na medida em que, nas palavras de Bauman, a internet veio para *substituir o trabalho de erguer-se e sair da invisibilidade e do esquecimento*¹⁸⁴, utilizam-se delas os indivíduos para se firmarem no campo social, o que fazem não pela coerção panóptica, mas sim pela sedução e tentação produzida pelo mercado e, ao fim e ao cabo, pela própria lógica da vida hodierna, entusiasmada com a presença – e a divulgação dessa presença – no mundo sinóptico digital¹⁸⁵.

Há, assim, um envolvimento voluntário dos cidadãos com a própria vigilância. Em uma sociedade tida como confessional¹⁸⁶, a “morte do anonimato”, por cortesia da internet, revela que submetemos à matança nossos direitos de privacidade por vontade própria¹⁸⁷. Ou talvez apenas consintamos em perder a privacidade como

tentação e sedução assumindo as funções antes desempenhadas pela regulação normativa; o sustento e o aguçamento dos desejos tomam o lugar do policiamento, caro e gerador de discórdias; portanto, as torres de vigilância (tal como toda a estratégia destinada a estimular a conduta desejável e eliminar a indesejável) foram privatizadas, enquanto o procedimento de emitir permissões para a construção de muralhas foi desregulamentado. Em vez de a necessidade caçar suas vítimas, agora é tarefa dos voluntários caçar as oportunidades de servidão (o conceito de “servidão voluntária” cunhado por Étienne de la Boétie teve de esperar quatro séculos até se transformar no objetivo comum da prática gerencial)”. (BAUMAN, 2014, p. 72-73).

¹⁸⁴ Atualizando o *cogito*, de Descartes, assim o reescreve o sociólogo polonês: “sou visto (observado, notado, registrado), logo existo”. (BAUMAN, 2014, p. 121).

¹⁸⁵ Nesse sentido, retoma-se novamente Bauman: “Nunca ocorreria a Bentham que tentação e sedução fossem as chaves da eficiência do pan-óptico em produzir um comportamento desejável. Não havia cenoura, apenas uma vareta na caixa de ferramentas do pan-óptico. A vigilância ao estilo pan-óptico presume que o caminho para a submissão a uma oferta passa pela eliminação da escolha. Nossa vigilância empregada pelo mercado presume que a manipulação da escolha (pela sedução, não pela coerção) é o caminho mais seguro para esgotar as ofertas por meio da demanda. A cooperação não apenas voluntária, mas entusiástica, dos manipulados é o principal recurso empregado pelos sinópticos dos mercados de consumo”. (BAUMAN, 2014, p. 125).

¹⁸⁶ Sociedade confessional pode ser entendida como “aquela que se destaca por eliminar a fronteira que antes separava o privado do público, e por fazer da exposição pública do privado uma virtude e uma obrigação pública, varrendo da comunicação pública qualquer coisa que resista a ser reduzida a confidências privadas, juntamente com aqueles que se recusam a confidenciá-las” (BAUMAN, 2014, p. 37).

¹⁸⁷ Nesse contexto, Carissa Véliz nos ensina que, embora as redes sociais permitam uma comunicação irrestrita, a civilidade exige certo grau de moderação, tanto em relação ao que se compartilha sobre si mesmo, quanto às opiniões expressas, especialmente quando envolvem terceiros, e às questões que

preço razoável pelo que nos é oferecido em troca” (Zygmunt. Vigilância... p. 28.). Exemplos reais e importantes dessa situação pode ser dada pelas funcionalidades “lista de desejos”, mantidas, por exemplo, por empresas como a Amazon e o Walmart, em que o perfil do consumidor é criado por ele próprio, indicando para as empresas quais os produtos que estaria disposto a adquirir no futuro; e o botão “curtir”, do Facebook e Instagram, em que, após o titular do perfil social classificar os demais como “amigos” ou não, “seguidores” ou não, passa a mostrar para a rede social o que lhe agrada, permitindo – ou melhor – fornecendo um perfil de sua própria existência¹⁸⁸.

A *surveillance*, nesse contexto, deixou de ser mera vigilância, ou seja, um evento específico e dirigido contra determinados sujeitos, passando a constituir uma das características inevitáveis das sociedades contemporâneas. Diferentemente do romance *1984*, em que George Orwell nos apresenta a vigilância como amedrontadora e centralizada em um Estado totalitário, observamos hoje uma presença “amiga”, “transparente” da vigilância personalizada nas empresas privadas. Ao contrário de um opressor *Big Brother*, observamos a existência de várias, na expressão popularizada por Elias Jacob de Menezes Neto, *Little Sisters*¹⁸⁹ –

são levantadas. É irrealista e injusto esperar que as pessoas se comportem de maneira impecável em corpo, fala e pensamento em todos os momentos. Forçar as pessoas a compartilhar mais do que o fariam voluntariamente resultaria em um ambiente social mais tóxico do que se incentivássemos a prudência e a seleção cuidadosa do que é compartilhado na esfera pública. Uma cultura que promove a exposição indiscriminada nos instiga a compartilhar até mesmo nossos pensamentos mais sombrios, o que, por sua vez, pode criar conflitos desnecessários. Poupar uns aos outros das partes menos agradáveis de nossas vidas não é uma fraqueza, mas sim uma manifestação de cortesia (2021, p. 149).

¹⁸⁸ Acerca da voluntariedade no fornecimento dos dados pessoais e a assunção dessa tarefa aos indivíduos, brilhante a inferência de Zygmunt Bauman: “Em suma, tal como os caramujos transportam suas casas, os empregados do admirável novo mundo líquido moderno precisam crescer e transportar sobre os próprios corpos seus panópticos pessoais. Aos empregados e a todas as outras variedades de subordinados foram atribuídas a responsabilidade plena e incondicional de mantê-los em bom estado e garantir seu funcionamento ininterrupto (deixar seu celular ou iPhone em casa para dar um passeio, suspendendo a condição de permanentemente à disposição de um superior, é um caso de falha grave). Tentado pelos encantos dos mercados de consumo e assustados com a possibilidade de que a nova liberdade em relação aos chefes se desvaneça, juntamente com as ofertas de emprego, os subordinados estão tão preparados para o papel de autovigilantes que se tornam redundantes em relação às torres de vigilância do esquema de Bentham e Foucault”. (BAUMAN, 2014, p. 61).

¹⁸⁹ Jogo de palavras: Enquanto o *Big Brother* pode ser traduzido como *Grande Irmão*, a expressão *Little Sisters* pode ser traduzida como *Pequenas Irmãs*.

justamente a figura das empresas¹⁹⁰ que, voltadas a seus próprios interesses, captam e tratam dados pessoais¹⁹¹.

O maior exemplo dessa convivência entre interesses estatais e particulares na vigilância massiva e diuturna da sociedade, modelo por excelência da prática sofisticada da *surveillance* na contemporaneidade, se refere às técnicas de espionagem estadunidense reveladas pelo ex-agente da Agência de Segurança Nacional dos Estados Unidos, Edward Snowden¹⁹². Consoante exposto pelo ex-analista de sistemas, toda a comunicação desejável era armazenada pelos servidores estatais, tornando-se passível de tratamento. Essa técnica de vigilância difere daquelas apresentadas pela teoria tradicional, visto que ultrapassa quaisquer limites físicos da observância humana para relegar a dispositivos eletrônicos a tarefa de auscultar os indivíduos em diferentes plataformas de comunicação.

¹⁹⁰ Consoante expõe Elias Jacob de Menezes Neto: “O problema real da *surveillance* no mundo contemporâneo é a coleta de dados por parte da iniciativa privada. Ou seja, ao invés de ser uma ferramenta de um *Big Brother* opressor, a *surveillance* contemporânea é utilizada por uma infinidade de “*Little Sisters*”, cujo objetivo principal é conhecer melhor o indivíduo consumidor através da invasão de todas as esferas da sua vida. A *surveillance* deixa de ser uma prática exclusivamente estatal e passa a ser um traço caracterizador da sociedade em que vivemos. (JACOB NETO, 2014, p. 15-16.)

¹⁹¹ Isso não significa, repise-se, que a ingerência governamental nos dados pessoais, para fim de controle e categorização social, seja algo diminuído, com relevância menor do que teria no âmbito do romance: o panóptico enquanto controle central está, consoante sobredito, *ciborguizado, forte e bem de saúde*. Entretanto, sua existência é compartilhada com outros polos captadores de dados pessoais – e, portanto, de vigilância. Elias Jacob de Menezes Neto, nesse sentido, salienta que “é fundamental lembrar que a manutenção da ordem social em Oceania ocorria através do elemento centralizador do Estado no controle de toda a informação. Contudo, ainda que governos centralizem enorme capacidade de coletar e processar dados – basta lembrar o “efeito Snowden” –, os dois traços mais importantes da *surveillance* atual são a descentralização e a mudança das suas finalidades – antes, para otimizar a produção, hoje, para aumentar o consumo. O grau de refino e de imbricação – novamente, como pode ser visto nas parcerias entre iniciativa privada e poder público no caso Snowden – entre público, privado, nacional e internacional impedem impõem o questionamento sobre até que ponto faz sentido a dicotomia centralizado/descentralizado.” (JACOB NETO, 2014, p. 13).

¹⁹² Edward Joseph Snowden, ex-analista de sistemas que trabalhou para a Agência de Segurança Nacional dos Estados Unidos (NSA), revelou ao público, por meio de entrevistas concedidas no ano de 2013, um elaborado esquema de interceptação e armazenamento de dados pelo governo dos Estados Unidos e outros estados soberanos. Esses fatos, divulgados em diversos periódicos e detalhados no livro “Sem Lugar Para Se Esconder” (2014), escrito por Glenn Greenwald com base nas revelações de Snowden, expuseram a complexidade e o alcance desse programa de espionagem. Em abril de 2013, Greenwald foi contatado pela cineasta e documentarista estadunidense Laura Poitras, que havia recebido e-mails anônimos relatando a existência de um programa de espionagem dos EUA. Isso levou ao encontro pessoal entre Poitras e Greenwald em Nova York, onde Poitras compartilhou informações sobre os documentos ultrassecretos em sua posse. Na semana de 20 de maio de 2013, Greenwald foi contatado diretamente por Edward Snowden, a fonte dos vazamentos, e iniciou uma conversa protegida por criptografia. Snowden compartilhou suas intenções de iniciar um debate mundial sobre privacidade, liberdade na internet e vigilância estatal, apesar de saber que isso colocaria sua vida em risco. Ele expressou seu medo de que as pessoas pudessem ignorar as revelações, tornando seu sacrifício em vão. A partir desse ponto, Greenwald e Poitras começaram a revelar o maior programa de interceptação e armazenamento de dados pessoais da história. (GREENWALD, 2014).

Snowden¹⁹³. forneceu ao jornalista Glenn Greenwald, no primeiro encontro pessoal entre os dois¹⁹⁴, a fim de comprovar suas alegações, uma pequena parte dos documentos que possuía, com a ressalva de que esses documentos eram apenas a "ponta do iceberg". Os documentos classificados como ultrassecretos incluíam informações sobre programas de coleta de dados de empresas como *Microsoft*, *Yahoo!*, *Google*, *Facebook*, *AOL*, *Skype*, *Youtube* e *Apple*, bem como um manual de treinamento para agentes da NSA. Esses documentos revelaram a extensão da coleta de dados pessoais, incluindo endereços de e-mail, dados de localização de IP, números de telefone, conteúdo de e-mails e metadados telefônicos. (GREENWALD, 2014, p. 29-30)

A cronologia dos eventos e incidentes que culminaram na revelação de um vasto programa de espionagem mantido principalmente pelos Estados Unidos constituem menos o nosso foco do que as "ferramentas em si", ou seja, os mecanismos empregados pelo governo dos Estados Unidos para efetuar a coleta e o tratamento de dados pessoais. Há uma variedade de aplicações para esses fins, e aqui detalharemos aquelas que têm maior relevância e impacto, tanto qualitativamente quanto quantitativamente, nas operações de vigilância do Estado.

É importante destacar que todos esses programas de vigilância têm em comum sua centralização na Agência de Segurança Nacional (NSA). Os objetivos dessa agência¹⁹⁵ – apresentados, ortodoxamente, como vinculados à Inteligência de

¹⁹³ Edward Snowden nasceu na Carolina do Norte, em 21 de junho de 1983, e cresceu em Maryland, em uma família de classe média baixa de funcionários públicos federais. Ele teve uma educação pouco convencional e ingressou no exército dos EUA aos 20 anos, antes de trabalhar para a CIA e, posteriormente, para a NSA. Ele passou a maior parte do tempo em Genebra, Suíça, antes de retornar aos EUA e decidir se tornar um delator.

¹⁹⁴ Glenn Greenwald viajou para Nova York para se encontrar com Laura Poitras e, juntos, viajaram para Hong Kong, em junho de 2013, para se encontrarem com Snowden. O encontro ocorreu no Hotel Mira, em 3 de junho de 2013, revelando Snowden como um homem jovem de 29 anos. Greenwald começou a coletar informações sobre a vida e a carreira de Snowden, bem como sobre os programas de espionagem dos EUA.

¹⁹⁵ Criada em 4 de novembro de 1952, a própria agência assim apresenta seus objetivos: "A Agência de Segurança Nacional/Serviço Central de Segurança (NSA/CSS) lidera o Governo dos EUA em criptologia, que engloba tanto os serviços de inteligência de sinais (SIGINT) como os produtos e serviços de garantia de informação (IA), e permite a Operação de Rede de Computadores (CNO), de maneira a alcançar uma vantagem decisiva para a Nação e nossos aliados sob todas as circunstâncias". (Original em inglês: *The National Security Agency/Central Security Service (NSA/CSS) leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO) in order to gain a decision advantage for the Nation and our allies under all circumstances*). Disponível em: <https://www.nsa.gov/about/mission-strategy/>. Acesso em: 30 ago. 2023.

Sinais (SIGINT), incluindo interceptação e criptoanálise de conteúdos nocivos aos interesses dos Estados Unidos – após as revelações de Snowden, foram desnudados, revelando-se sua principal missão: a captura e o armazenamento de dados pessoais, fornecendo subsídios para a atuação política dos EUA em várias áreas de interesse.

Antes de entrarmos na análise detalhada dos programas de vigilância, é crucial compreender que a atuação desses programas não é uniforme em relação a todos os países. Isso ocorre porque os Estados Unidos, juntamente com outros quatro países, formam uma aliança conhecida como "*Five Eyes*". Nesse contexto, eles auxiliam mutuamente nas atividades de espionagem. A NSA mantém três tipos diferentes de relações com países estrangeiros: cooperação abrangente com os membros do *Five Eyes*, cooperação focada com outros países e espionagem rotineira de alguns países sem cooperação (*Ibidem*, p. 126).

Dentro do *Five Eyes*, o aliado mais próximo da NSA é a Central de Comunicações do Governo Britânico (GCHQ). De acordo com Snowden, os Estados Unidos teriam pago substancialmente (no mínimo 100 milhões de libras) para ter acesso e influência nos programas de coleta de dados geridos pelo GCHQ (*Idem*).

As conferências anuais de Desenvolvimento de Sinais são um exemplo das interações promovidas por esses países, onde apresentam resultados da expansão de seus programas de vigilância. Além disso, programas específicos de vigilância foram criados e mantidos pelos países membros desse grupo, como o sistema *Tempora*, desenvolvido pela GCHQ. Esforços para quebrar a criptografia também eram frequentemente apoiados pela agência britânica, com a participação da NSA (*Idem*).

Programas de espionagem mantidos pelo Canadá e pela Austrália também merecem destaque, com exemplos de atividades de espionagem direcionadas a governos estrangeiros e solicitações da Austrália para que a NSA intensificasse a vigilância sobre seus próprios cidadãos considerados suspeitos por seu governo.

Antes, ainda, de prosseguirmos com a análise dos programas de vigilância, vale a pena mencionar o papel do *Foreign Intelligence Surveillance Act* de 1978 (FISA) na expansão e manutenção das atividades de coleta de dados pelos Estados Unidos. Sob essa legislação, a NSA pode monitorar o conteúdo das comunicações dos americanos sem mandados individuais, desde que essas comunicações envolvam

cidadãos estrangeiros sob monitoramento. É notável que o Tribunal da FISA tenha autorizado a grande maioria das solicitações de vigilância apresentadas pela NSA, o que levanta questões sobre sua eficácia como mecanismo de supervisão¹⁹⁶.

Por fim, é importante classificar as informações coletadas pelos órgãos de vigilância em duas categorias principais: "conteúdo" e "metadados". O conteúdo refere-se à escuta de chamadas telefônicas, leitura de e-mails e chats, bem como o acesso às atividades de navegação na internet, como históricos de navegação e buscas. Os metadados incluem informações sobre essas comunicações, como remetentes, destinatários, horários e locais (*Ibidem*, p. 139).

A NSA coleta ambas as categorias de informações, embora afirme que a maioria dos dados seja do tipo "metadados". No entanto, essa forma de vigilância pode ser tão invasiva quanto a outra, uma vez que o mapeamento de contatos telefônicos, duração de chamadas e detalhes de e-mails fornece uma visão detalhada das vidas e preferências das pessoas, bem como informações pessoais e íntimas¹⁹⁷. Isso é conhecido como "*profiling*" e representa uma mudança qualitativa no tratamento de dados pessoais¹⁹⁸.

Os principais programas de vigilância¹⁹⁹ incluem o PRISM, que envolveu empresas de internet; BOUNDLESS INFORMANT, que rastreia chamadas e e-mails

¹⁹⁶ O Tribunal da FISA autoriza quase que a totalidade das solicitações de vigilância apresentadas pela NSA: desde a sua criação, de 1978 a 2002, o Tribunal rejeitou o impressionante número de zero solicitações do governo, aprovando muitos milhares; na década compreendida entre 2002 e 2012, foram rejeitadas onze solicitações oficiais, e aprovados mais de 20 mil pedidos. Mais especificamente quanto aos anos de 2011 e de 2012, o Tribunal aceitou 1.676 e 1.788 solicitações, respectivamente, alterando parcialmente, em 2011, o conteúdo de 30 solicitações, e, em 2012, de quarenta, não negando qualquer deles. (*Ibidem*, p. 135-136).

¹⁹⁷ Nesse sentido o relevante exemplo dado por Stefano Rodotà: "Consideremos, por exemplo, o caso das coletas de dados utilizada pelos poderes públicos para tomar decisões que dizem respeito a intervenções de diversos gêneros ou a programas de investimento. Sustenta-se que estas coletâneas, contendo exclusivamente dados agregados, não são perigosas para a privacidade, já que para esses dados não seriam necessários controles especiais ou o reconhecimento aos indivíduos de um direito de acesso. Porém, é fácil objetar que mesmo as coletâneas de dados anônimos podem ser manipuladas de forma gravemente lesiva aos direitos dos indivíduos: tenha-se em mente o uso que pode ser feito dos dados, agregados, que digam respeito a uma minoria racial ou linguística; ou às consequências de uma decisão política ou econômica tomada justamente com base na análise de dados anônimos". (RODOTÁ, 2008, p. 32).

¹⁹⁸ Sobre o tema, ver DONEDA, 2020, p. 173.

¹⁹⁹ Além dos três principais programas de vigilância adiante tratados, Greenwald listou tantos outros *softwares* utilizados pela NSA para captura e tratamento de dados pessoais, a exemplo do TARMAC, SHELLTRUMPET (que, em dezembro de 2012, processou seu trilionésimo registro), BLARNEY, FAIRVIEW, OAKSTAR, STORMBREW, TEMPORA, MUSCULAR e STATEROOM. Todos eles possuem grande importância e denotam a preocupação da NSA em desenvolver aparatos de coleta de dados pessoais; esmiuçá-los, entretanto, desborda dos objetivos do presente trabalho.

em todo o mundo; e X-KEYSCORE, que permite monitoramento em tempo real. Esses programas têm acesso a grandes quantidades de dados pessoais, levantando preocupações com a privacidade.

O programa de espionagem conhecido como PRISM permitiu que a Agência de Segurança Nacional (NSA) dos Estados Unidos adquirisse informações diretamente nos servidores de empresas de internet, incluindo *Microsoft, Yahoo!, Google, Facebook, PalTalk, AOL, Skype, YouTube* e *Apple*, de acordo com documentos divulgados por Edward Snowden. Embora as empresas tenham negado o acesso irrestrito a seus bancos de dados, há indícios de que o PRISM desempenhou um papel significativo na coleta de dados pessoais sem o consentimento dos usuários. Evidências como recursos legais negados ao *Yahoo!*, slides de Snowden demonstrando a interface do programa e o aumento substancial na coleta de dados pela NSA, especialmente em servidores do *Skype, Facebook* e *Google*, indicam a importância e a eficácia do PRISM como um programa de espionagem. Algumas empresas não concordaram com o uso do sistema, como o *Yahoo!*, e outras adaptaram seus sistemas para serem compatíveis com as atividades do PRISM, embora não tenham sido especificadas por Snowden. (*Ibidem*, p. 117-118).

O programa de vigilância BOUNDLESS INFORMANT²⁰⁰, por sua vez, desempenha um papel significativo na coleta e contabilização precisa de todas as chamadas e e-mails em todo o mundo. Documentos obtidos da NSA revelam que o programa é capaz de quantificar bilhões de registros diariamente, demonstrando sua magnitude impressionante. Em um mês, uma unidade da NSA, chamada *Global Access Operation*, coletou dados de mais de 3 bilhões de chamadas e e-mails que passaram pelo sistema de telecomunicações dos Estados Unidos. Considerando as comunicações globais, a mesma unidade coletou incríveis 97 bilhões de e-mails e 124 bilhões de chamadas telefônicas em apenas trinta dias, incluindo dados da Alemanha e Índia, e metadados coletados em parceria com governos francês, espanhol e italiano. Além disso, foi revelado que a *Verizon* – uma das maiores operadoras de telefones móveis dos Estados Unidos²⁰¹ – foi instruída pelo Tribunal da FISA a fornecer à NSA informações sobre as ligações de seus clientes norte-americanos, os

²⁰⁰ Em tradução livre: *informante ilimitado*, ou, ainda, *informante sem fronteiras*.

²⁰¹ VERIZON. Disponível em: <http://www.verizon.com/about/our-company/who-we-are>. Acesso em: 01 fev. 2017.

"metadados de telefonia." Essas revelações apontam para o objetivo declarado do Estado de vigilância dos EUA de eliminar a privacidade eletrônica em escala global²⁰², coletando, armazenando e monitorando todas as comunicações eletrônicas de todas as pessoas, refletindo um sistema de vigilância em larga escala que busca abranger todas as comunicações eletrônicas (*Ibidem*, p. 99-100).

Por fim, o programa X-KEYSCORE, usado como o principal meio de coleta, classificação e pesquisa de informações e conteúdo de e-mails, históricos de navegação, históricos de busca e chats pela NSA, representa um avanço significativo nos poderes de vigilância da agência. Este programa permite o monitoramento em tempo real das atividades online de indivíduos, possibilitando a observação de dados no momento em que são gerados e transmitidos. Os analistas da NSA podem pesquisar as bases de dados do sistema por endereço de e-mail, número de telefone e endereço IP, bem como recuperar documentos e imagens anexados a mensagens. Além disso, o X-KEYSCORE facilita a criação de listas abrangentes de visitas a sites específicos feitas a partir de qualquer computador. Este software permite a coleta quase irrestrita de uma ampla gama de informações pessoais, com documentação indicando o recebimento diário de mais de 20 terabytes de dados e, em um mês, 41 bilhões de registros por uma única unidade da NSA. Uma característica notável do programa é a facilidade com que os analistas podem acessá-lo e realizar pesquisas, sem a necessidade de aprovação de supervisores ou autoridades superiores, simplesmente preenchendo um formulário para justificar a vigilância e obter as informações desejadas, incluindo a leitura do conteúdo de e-mails, o que evidencia o potencial intrusivo e amplo do sistema (*Ibidem*, p. 162-169).

Os Estados Unidos têm utilizado agências como a NSA para fins de espionagem no âmbito das estratégias de planejamento de outros países, especialmente durante discussões sobre comércio e economia. Essa prática visa a proporcionar uma vantagem significativa para a indústria norte-americana. Além

²⁰² Essa capacidade de interpretação e contabilização dos dados levou Greenwald, inclusive, a afirmar, em relação ao BOUNDLESS INFORMANT: "Considerando em sua totalidade, o acervo de Snowden levava, em última instância, a uma conclusão bem simples: o governo dos Estados Unidos construiu um sistema cujo objetivo é a completa eliminação da privacidade eletrônica do mundo inteiro. Longe de ser uma hipérbole, esse é o objetivo literal e explicitamente declarado do Estado de vigilância: coletar, armazenar, monitorar e analisar todas as comunicações eletrônicas de todas as pessoas ao redor do mundo. A agência se dedica a uma missão maior: evitar que qualquer comunicação eletrônica, por mais ínfima que seja, fuja ao seu alcance sistemático". (*Ibidem*, p. 101).

disso, o lobby das empresas de vigilância defensiva é altamente influente, já que essas empresas buscam alocar recursos governamentais em seus próprios lucros, aproveitando o temor relacionado à era pós-11 de setembro.

A justificativa central para os programas de vigilância mantidos pelos Estados Unidos é a segurança. Sob o pretexto de proteger o país contra atos de terrorismo, a vigilância se estende até mesmo aos "cidadãos comuns", aumentando o poder das entidades que coletam dados pessoais. Glenn Greenwald argumenta que um dos principais argumentos para justificar a vigilância é a divisão entre "pessoas boas" e "pessoas más". A ideia é que as autoridades usam seus poderes de vigilância apenas contra as pessoas "más", aquelas que estão "fazendo algo errado". No entanto, essa percepção simplista muitas vezes leva as pessoas a aceitarem o abuso de poder, pois a dissidência e qualquer forma de contestação podem ser interpretadas como "fazer algo errado" (*Ibidem*, p. 195.).

Desde os ataques de 11 de setembro de 2001, os Estados Unidos têm adotado um discurso centrado na segurança. No entanto, como mencionado, os programas de vigilância vão além da mera preocupação com o terrorismo. Não se pode afirmar que a interceptação das comunicações da Petrobras, a espionagem durante negociações econômicas e o monitoramento de líderes de países aliados estão relacionadas ao terrorismo (*Ibidem*, p. 214).

A narrativa ora apresentada poderia fazer parecer, outrossim, que o governo estadunidense, em sua sanha de controlar tudo e todos por meio de técnicas de *surveillance*, agiria de forma truculenta para com as empresas outrora mencionadas – responsáveis, muitas vezes, por fornecer ao Estado a matéria-prima que capturaram, ao seduzirem os usuários de suas funcionalidades digitais. No entanto, o que se percebe, no mais das vezes, é uma mansa condescendência dessas empresas: mesmo porque elas se beneficiam largamente da mesma atividade, voltada à captura e tratamento de dados além do desejado por qualquer sociedade que preze pela privacidade²⁰³.

²⁰³ Conforme escreve Greenwald: "Embora a NSA seja oficialmente um órgão público, mantém incontáveis parcerias com empresas do setor privado, e muitas de suas principais funções foram terceirizadas. A agência em si tem em torno de 30 mil funcionários, mas também mantém sob contrato cerca de 60 mil funcionários de companhias particulares, que muitas vezes prestam serviços essenciais. O próprio Snowden não era funcionário da NSA, mas sim da Dell Corporation e da grande prestadora de serviços da área de defesa Booz Allen Hamilton. No entanto, assim como outros

Os fatos revelados por Snowden, portanto, vão ao encontro das reflexões promovidas por Véliz. A captura e análise de dados têm um papel significativo na sociedade, afetando desde indivíduos comuns até decisões políticas importantes. Essa atividade pode influenciar o comportamento das pessoas, moldar suas escolhas e até determinar resultados eleitorais, destacando a importância de proteger a privacidade e regulamentar o uso de dados pessoais.

No século XXI, a vigilância, portanto, não é mais exclusividade de um ditador ou de uma agência governamental, mas está presente em todas as partes da sociedade. À capacidade massiva de captação e tratamento de dados pessoais, possibilitada pelas poderosas tecnologias que, diariamente, surgem ao redor do globo e são utilizados pelo aparato dominante-repressivo do Estado, alia-se outra: “amiga”, “transparente” da vigilância personalizada nas empresas privadas, direcionadas não às pessoas específicas, em tempo certo e espaços determinados – mas a todos os indivíduos, o tempo todo, em todo lugar. O que sustenta, portanto, a inadequação da vigilância para traduzir a complexidade do fenômeno contemporâneo referido como *surveillance*.

E por fim, a quarta face das “sociedades envenenadas” pela toxicidade dos dados pessoais é representada pelas ameaças à segurança dos indivíduos. Com efeito, os dados pessoais, ao longo da história, provaram ser suscetíveis a abusos graves e mortais. Um exemplo notável desses abusos ocorreu durante a Segunda Guerra Mundial, quando o regime nazista utilizou dados pessoais para identificar e

prestadores de serviços de empresas privadas, trabalhava dentro das instalações da NSA, executando uma de suas principais funções e com acesso a seus segredos. Segundo Tim Shorrock, que há muito tempo estuda a relação da NSA com o setor privado, “70% do nosso orçamento de inteligência nacional estão sendo gastos no setor privado”. Quando Michael Hayden afirmou que “a maior concentração de poder cibernético do planeta está no cruzamento da Avenida Baltimore com a Rodovia 32, em Maryland”, Shorrock comentou que “ele não estava se referindo à NSA em si, mas sim ao parque empresarial situado a cerca de 1,5 quilômetro do gigantesco edifício preto que abriga a sede da NSA em Fort Meade, Maryland. É ali que todas as grandes prestadoras de serviços da NSA, da Booz à SAIC, passando pela Northrop Grumman, executam o trabalho de vigilância e inteligência para a agência”. Além das prestadoras de serviços de inteligência e defesa, essas parcerias corporativas incluem também algumas das maiores e mais importantes empresas de internet e telecomunicações, justamente aquelas que processam a maior parte das comunicações do mundo e podem facilitar o acesso a dados pessoais”. (GREENWALD, 2014, p. 108).

perseguir judeus em territórios ocupados²⁰⁴. A comparação entre a abordagem holandesa e francesa em relação aos dados populacionais ilustra essa diferença²⁰⁵.

Esses exemplos históricos destacam como a coleta excessiva e o mau uso de dados pessoais podem ter consequências mortais. A privacidade desempenhou um papel vital na proteção de vidas na França. Imagine agora um regime autoritário contemporâneo com acesso a dados pessoais em tempo real, como localização, biometria facial, preferências políticas e religiosas. Essa situação poderia levar, na forma refletida por Carissa, ao surgimento de regimes invencíveis (*Ibidem*, p. 160).

Essas histórias reais do passado nos ensinam a importância de proteger os dados pessoais e a privacidade. Precisamos regular os dados pessoais de maneira adequada e aprender com os erros cometidos no passado. Não podemos permitir que os dados pessoais envenenem indivíduos, instituições e sociedades, como o amianto envenenou o ambiente. Ainda temos a oportunidade, conforme alerta Carissa, de

²⁰⁴ A obra mais importante sobre o assunto – *IBM e o Holocausto: a aliança estratégica entre a Alemanha nazista e a mais poderosa empresa americana* – referenciada, inclusive, por Carissa Véliz, foi escrita por Edwin Black, no ano de 2001. Entre as várias passagens, destaca-se: “8 de janeiro de 1934. Num canto da vasta área de operações com cartões perfurados, no grande complexo censitário de Alexanderplatz, em Berlim, onde a luz da manhã se infiltrava pelos fundos, através de uma fileira de janelas paralelas, várias dezenas de funcionários do Escritório Estatístico Prussiano se misturavam com líderes do Partido Nazista, envergando uniforme completo, e com o pessoal da Dehomag, trajando seus melhores ternos, para solenemente conhecer a próxima revolução em processamento de dados e a nova aliança com a International Business Machines. Mãos juntas, reverentemente, por trás, abaixo da cintura, ou pela frente, mais ou menos na altura da fivela do cinto; ombros e braços tocando-se, num clima de camaradagem, os presentes se reuniam para celebrar aquele dia, quando a Alemanha revelaria ao mundo sua própria fábrica de produção de máquinas Hollerith. O Presidente do Escritório Estatístico Prussiano, Dr. Höpker, proferiu breves observações, recorrendo aos eufemismos e às divagações cristalinas do dia. “...A força irresistível do governo nacional-socialista ... demanda resultados [censitários] com mais rapidez do que nunca”, declarou, acrescentando: “Os estatísticos alemães compreendem essa impaciência ...”. Em seguida, explicou exatamente como funcionava o processo de cartão perfurado, convertendo as anônimas massas alemãs em listagens de nomes individuais, classificados por raça e religião, além de numerosas outras características. (BLACK, 2001, p. 94-95).

²⁰⁵ Nos Países Baixos, Jacobus Lambertus Lentz, inspetor dos Registros Populacionais, propôs um sistema de identificação pessoal antes da invasão nazista, que obrigaria todos os cidadãos a portar um cartão de identidade. Esse sistema foi posteriormente adotado pelos nazistas e usado para identificar judeus, marcando-os com a letra "J". As máquinas Hollerith, da IBM, foram usadas para expandir os registros populacionais e facilitar o rastreamento de pessoas. Na França, por outro lado, não havia registros detalhados de religião e a coleta de dados era menos extensiva. O chefe do Escritório Geral de Estatísticas da França, Henri Bunle, deixou claro que a França não tinha informações precisas sobre a população judaica. A falta de dados detalhados sobre religião e a ausência de máquinas Hollerith dificultaram o rastreamento de judeus na França. A diferença entre esses dois casos é notável. Nos Países Baixos, onde os dados pessoais eram extensos e detalhados, a taxa de mortalidade dos judeus foi de 73%, enquanto na França, onde a privacidade era mais preservada, a taxa foi de 25%. Refugiados judeus que escaparam do registro também tiveram uma taxa de mortalidade mais baixa nos Países Baixos. (VÉLIZ, 2021, p. 157-158).

corrigir nosso curso atual em relação aos dados pessoais e à privacidade, antes que seja tarde demais²⁰⁶.

Em razão de todo o exposto acerca da discussão sobre a toxicidade dos dados pessoais e as implicações para a privacidade e a democracia, a realidade brasileira exige uma análise crítica que vá além da simples importação de conceitos e marcos regulatórios estrangeiros. O Brasil, como nação em desenvolvimento e parte do Sul Global, enfrenta desafios particulares no cenário global de proteção de dados. A questão aqui não é apenas a proteção individual contra violações de privacidade, mas também a proteção da soberania digital e a prevenção do colonialismo de dados — fenômeno em que nações e corporações mais poderosas extraem e exploram dados de países menos desenvolvidos, perpetuando assimetrias globais, e que representam uma toxicidade adicional e específica relacionada à vivência periférica relacionada aos interesses na predação e emprego de dados pessoais.

Neste contexto, a ANPD deve desempenhar um papel proativo na proteção contra a exploração econômica e política dos dados brasileiros. A emissão de decisões de adequação não é um mero exercício técnico, mas uma defesa necessária contra o colonialismo de dados, em que corporações multinacionais e Estados estrangeiros detêm um controle desproporcional sobre os dados de populações vulneráveis. Para isso, a ANPD precisa estabelecer critérios rigorosos para avaliar as condições sob as quais os dados podem ser transferidos e garantir que qualquer transferência internacional respeite os padrões de proteção estabelecidos pela Lei Geral de Proteção de Dados (LGPD). Algo que não se encontra devidamente tratado e tutelado no âmbito da Resolução CD/ANPD nº 19/2024.

A relevância dessa postura fica ainda mais evidente ao se considerar que o Brasil, como parte do Sul Global, tem uma longa história de exploração por parte de potências estrangeiras, tanto no âmbito econômico quanto político. No cenário digital contemporâneo, os dados pessoais se tornaram o novo recurso a ser explorado, e sem uma regulação robusta e ativa por parte da ANPD, o país corre o risco de repetir

²⁰⁶ E tenhamos, por fim, que endossar a opinião da Filósofa da Universidade de Oxford, para quem: “A economia da vigilância foi longe demais. Ela abusou de nossos dados pessoais de muitas maneiras, muitas vezes. E a quantidade e a sensibilidade dos dados comercializados tornam esta grande experiência perigosa demais para continuar. Temos de pôr um fim ao comércio de dados pessoais. A economia de dados tem de acabar pois está em desacordo com as democracias livres, igualitárias, estáveis e liberais”. (VÉLIZ, 2021, p. 163).

antigos padrões de dependência e subserviência. Assim, a emissão de decisões de adequação deve ser vista como um instrumento fundamental para a proteção dos direitos dos cidadãos brasileiros e para a preservação da soberania nacional na era digital.

3.2 Colonialismo de dados

Na esteira dos estudos sobre a *colonialidade*, o colonialismo de dados surge como uma nova forma de dependência no capitalismo contemporâneo, em que práticas predatórias tradicionais do colonialismo histórico são agora aplicadas ao controle de dados pessoais captados e tratados em ambiente digital.

Os estudos sobre a *colonialidade* investigam o modo como as relações de poder coloniais continuam a moldar as estruturas globais, mesmo após o fim formal do colonialismo. Esses estudos, iniciados por teóricos como Aníbal Quijano, partem do conceito de "colonialidade do poder" para descrever a continuidade da dominação social, política, econômica e epistêmica imposta pelo colonialismo²⁰⁷. A colonialidade não se limita à presença territorial dos impérios, mas persiste nas divisões de classe e raça, nos modos de produção econômica e nas formas de conhecimento, com impacto duradouro sobre os povos historicamente subjugados, especialmente na América Latina, África e Ásia.

O *giro decolonial*, por sua vez, é uma proposta teórica e prática que busca desafiar e romper com a hegemonia eurocêntrica nas formas de conhecimento e nos modos de entender o mundo. Teóricos como Walter D. Mignolo e Catherine Walsh defendem que o *giro decolonial* consiste em "desobedecer" às epistemologias e instituições do Norte Global, substituindo-as por perspectivas e saberes provenientes dos povos colonizados²⁰⁸. Essa abordagem propõe epistemologias que se alinham

²⁰⁷ A "colonialidade do poder" foi abordada por Aníbal Quijano, com ênfase em trabalhos como: QUIJANO, Aníbal. Colonialidade do poder, eurocentrismo e América Latina. *In*: LANDER, Edgardo (Org.). **A colonialidade do saber: eurocentrismo e ciências sociais: perspectivas latino-americanas**. Buenos Aires: CLACSO, 2005. p. 117-142.

²⁰⁸ Para uma incursão aprofundada sobre o *giro decolonial*, ver: WALSH, Catherine. **La insubordinación fundante: América Latina y el giro decolonial**. Quito: Universidad Andina Simón Bolívar, Ediciones Abya-Yala, 2012. MIGNOLO, Walter D. **Desobediência epistêmica: a opção decolonial e o significado de identidade no pensamento crítico latino-americano contemporâneo**. *In*: CANDAU, Vera M. (org.). **Globalização e educação: desafios para políticas e práticas pedagógicas**. São Paulo: Cortez, 2015. p. 191-225. LANDER, Edgardo (Org.). **A colonialidade do saber:**

com as histórias, culturas e necessidades dos povos marginalizados, promovendo novas práticas de resistência e emancipação que valorizam conhecimentos locais e plurais, em contraposição à universalidade imposta pela modernidade ocidental.

Tanto o estudo sobre a *colonialidade* quanto o *giro decolonial* tem como ponto central a crítica às estruturas de poder e conhecimento estabelecidas pela colonialidade, ou seja, o legado do colonialismo que perdura nas práticas culturais, políticas, sociais e econômicas atuais. Essa perspectiva propõe uma revisão crítica do colonialismo além de sua presença territorial direta, focando em como ele persiste em formas de dominação e subordinação que ultrapassam os contextos históricos de colonização formal.

O grande teórico responsável pelos estudos sobre a *colonialidade* chama-se Aníbal Quijano (1928-2018), sociólogo e teórico peruano, amplamente reconhecido por seu trabalho em temas como a *colonialidade*, a dependência e a desigualdade social na América Latina²⁰⁹. Sua contribuição mais significativa para o campo das ciências sociais é justamente o conceito de “colonialidade do poder,” desenvolvido para compreender como as hierarquias estabelecidas durante a colonização

eurocentrismo e ciências sociais: perspectivas latino-americanas. Buenos Aires: CLACSO, 2005. MIGNOLO, Walter D. **The darker side of Western modernity: global futures, decolonial options.** Durham: Duke University Press, 2011.

²⁰⁹ Quijano trabalhou intensamente na América Latina e foi uma figura chave no desenvolvimento do pensamento decolonial, inspirando uma nova geração de intelectuais e ativistas a questionarem as imposições de um sistema global de conhecimento e poder dominado por perspectivas eurocêntricas. Para Quijano, a colonialidade não se limitava às práticas de dominação territorial, mas englobava relações complexas de poder que estruturam as identidades, os modos de produção e as epistemologias. Assim, ele propôs que as divisões de raça, que foram construídas e naturalizadas durante o período colonial, permanecem presentes, influenciando as relações sociais e econômicas entre o Norte e o Sul Global. Publicou extensivamente sobre os impactos da colonialidade nas práticas econômicas e nas instituições modernas, argumentando que a modernidade e o capitalismo estão profundamente enraizados nas dinâmicas de poder colonial. Sua obra tornou-se uma referência central para teóricos que exploram a persistência de desigualdades estruturais e as formas de resistência necessárias para superá-las. A importância de Quijano reside, sobretudo, na forma como ele ajudou a transformar o debate sobre a descolonização e a emancipação, ampliando o escopo da crítica para incluir o próprio conhecimento e os modos de ver o mundo. Suas ideias não só desafiaram o pensamento hegemônico ocidental, mas também abriram caminho para epistemologias que valorizam as experiências, saberes e necessidades das populações marginalizadas. Os trabalhos de maior envergadura de Quijano sobre o tema, além dos já mencionados, incluem Quijano, Aníbal 1967 “Urbanización, cambio social y dependencia” em Cardoso, Fernando Henrique e Weffort, Francisco (eds.) **América Latina: Ensayos de interpretación sociológica** (Santiago de Chile: Editorial Universitaria); QUIJANO, Aníbal. América, el capitalismo y la modernidad nacieron el mismo día. ILLA (Lima) Nº 10, janeiro; Quijano, Aníbal 1992 “Colonialidad y modernidad/razionalidad” em Perú Indígena (Lima) v. 13, n. 29.

continuaram a influenciar as estruturas de poder global mesmo após o término formal do colonialismo²¹⁰.

Com efeito, em *Colonialidade do poder, eurocentrismo e América Latina*, Quijano argumenta que, no processo de constituição histórica da América, as diversas formas de controle e exploração do trabalho foram gradualmente unificadas em torno de um novo padrão de poder articulado pelo capitalismo. Essa estrutura englobou a escravidão, a servidão, o trabalho assalariado e outras modalidades, como a pequena produção mercantil e o sistema de reciprocidade, adaptando-as ao mercado mundial. Argumenta, nesse contexto, que a novidade dessa configuração não reside apenas na coexistência simultânea dessas formas de trabalho, mas na maneira pela qual elas foram subordinadas ao capital e ao mercado global. Cada uma delas, então, não era apenas e ingenuamente uma continuação de práticas históricas de controle do trabalho, mas uma transformação deliberada para atender ao novo sistema de produção e acumulação capitalista.

Esse padrão global de controle do trabalho e da produção estabeleceu-se de maneira singular e revolucionária, formando, pela primeira vez, uma estrutura de poder global. O capitalismo mundial, nesse contexto, não apenas organizou o trabalho em escala global, mas também deu ao capital uma posição de centralidade na configuração das relações sociais e econômicas. Isso significava que as diversas formas de trabalho – por diferentes que fossem – estavam agora integradas ao capital e ao mercado mundial, funcionando como um conjunto articulado de modos de

²¹⁰ Aníbal Quijano, apesar de baluarte dos estudos sobre a colonialidade, não é o único teórico a abordar as consequências persistentes da dominação colonial. Outros pensadores latino-americanos e caribenhos contribuíram significativamente para expandir e aprofundar essa abordagem, articulando o impacto duradouro da colonialidade em diversas esferas da sociedade. Walter Mignolo, outrora citado, por exemplo, ampliou o conceito com a ideia de “desobediência epistêmica,” defendendo que é necessário romper com as epistemologias eurocêntricas para construir conhecimentos que reflitam as realidades e vivências dos povos marginalizados. Catherine Walsh também se destacou ao explorar a relação entre a colonialidade e as práticas de resistência na América Latina, defendendo a criação de epistemologias que valorizem o saber local e promovam a autonomia dos povos historicamente subjugados. Frantz Fanon, por sua vez, em obras como *Pele Negra, Máscaras Brancas* (1952) e *Os Condenados da Terra* (1961), analisou as consequências psicológicas e culturais da colonização, destacando como a colonialidade desumaniza e aliena os sujeitos colonizados, e enfatizou a importância da resistência como meio de restaurar a dignidade e a identidade dos povos oprimidos. Lélia Gonzalez, por sua vez, introduziu uma perspectiva afro-latina ao analisar o impacto do racismo e do sexismo nas mulheres negras, especialmente no contexto brasileiro. Em sua obra *Por um Feminismo Afro-Latino-Americano* (1988), Gonzalez promove uma decolonização que inclui questões de gênero e raça em sua visão de “amefricanidade” — conceito que une a luta dos povos da América Latina à da diáspora africana.

exploração. Cada forma de trabalho, apesar de manter certas características próprias, passou a depender estruturalmente dessa nova configuração capitalista, que ditava o ritmo e a direção de seu desenvolvimento e transformações.

Paralelamente, Quijano aponta que o capitalismo mundial se articulou à colonialidade do poder por meio de uma divisão racial do trabalho, estabelecendo uma relação entre raça e função no mercado global. As identidades racializadas – construídas com base na ideia de inferioridade dos colonizados – foram associadas a papéis específicos dentro dessa estrutura de controle do trabalho, naturalizando uma hierarquia racial que determinava o lugar dos indivíduos e grupos dentro do sistema econômico. Enquanto os colonizadores, portanto, se posicionavam (se posicionam) no topo da hierarquia racial, ocupando papéis de controle e se beneficiando do produto do trabalho explorado, a condição subordinada dos colonizados – justificada, consoante sobredito, pela racialização de suas identidades – implicava (implica) a sujeição a posições de trabalho exploradoras e subalternas.

O aspecto racial ocupa, para o pensador sul-americano, portanto, um papel central em sua formulação teórica. Nesse sentido, argumenta que o surgimento da América e do capitalismo colonial/moderno resultou na criação de um novo padrão de poder mundial, que se vale da noção de desigualdade racial para sua imposição. Esse conceito de raça, surgido como justificativa para a dominação colonial, foi, segundo Quijano, uma construção mental que permitiu classificar a população de acordo com uma suposta inferioridade biológica. Essa construção não apenas sustentou as relações coloniais, mas moldou o eurocentrismo enquanto racionalidade que permeia todas as dimensões do poder global até hoje, superando em longevidade o próprio colonialismo territorial (QUIJANO, 2005, p. 117).

Quijano, ao destacar a América como o primeiro "espaço/tempo" da modernidade, identifica dois processos interligados que estruturaram esse novo padrão de poder. Primeiro, justamente a classificação racial da humanidade, na qual as diferenças fenotípicas entre conquistadores e conquistados foram transformadas em marcadores de uma suposta inferioridade biológica, justificando a subordinação dos povos colonizados. Segundo, a articulação das formas de controle do trabalho, recursos e produção em torno do capital e do mercado mundial, consolidando a exploração econômica no cerne das relações coloniais. Dessa maneira, o colonialismo

não apenas definiu os papéis econômicos, mas também criou novas identidades sociais — como “índios”, “negros” e “mestiços” —, enquanto termos como “espanhol” e “português” adquiriram conotações raciais. Com isso, a identidade racial passou a funcionar como uma forma de classificação social fundamental, na qual os não-europeus foram relegados a uma posição de subordinação (Ibidem, p. 118).

A Europa, portanto, ao se constituir como identidade autônoma e centro da modernidade, utilizou o conceito de raça para naturalizar as hierarquias entre europeus e não-europeus. Esse processo legitima e perpetua antigas práticas de superioridade e inferioridade, ao mesmo tempo que estabelece a raça como o critério primordial para a distribuição dos papéis e das posições sociais no novo padrão de poder – critério hierárquico que, segundo o pensador latino americano, provou ser um dos instrumentos de dominação social mais eficazes e duradouros na história.

Além disso, o conceito de raça fundamentou um regime de exclusão no qual o não-branco foi associado a traços de inferioridade que se estendiam ao nível cultural e intelectual²¹¹. Essa categorização imposta pelas estruturas de poder colonial afetou profundamente o desenvolvimento das sociedades dominadas, já que as características culturais e os valores dos povos colonizados passaram a ser vistos como inferiores e exóticos, afastando-os da legitimidade da “universalidade” eurocêntrica.

A partir dessa base, Quijano define o conceito de *colonialidade do poder*, importante em seu desenvolvimento teórico, como a lógica de dominação e subordinação que transcende as estruturas políticas coloniais, permeando até hoje as relações entre o centro e a periferia, e justificando as hierarquias globais sob o manto da modernidade. A raça, assim, não apenas ordenou o sistema colonial, mas estabeleceu um modo universal de classificação social que se tornou uma matriz de poder global, na qual o não-branco segue sendo classificado como inferior e, portanto, passível de exploração. Esse sistema transformou o racismo em um fenômeno

²¹¹ Nesse sentido, afirma Quijano que: “Na América, a ideia de raça foi uma maneira de outorgar legitimidade às relações de dominação impostas pela conquista. A posterior constituição da Europa como nova identidade depois da América e a expansão do colonialismo europeu ao resto do mundo conduziram à elaboração da perspectiva eurocêntrica do conhecimento e com ela à elaboração teórica da ideia de raça como naturalização dessas relações coloniais de dominação entre europeus e não-europeus. Historicamente, isso significou uma nova maneira de legitimar as já antigas ideias e práticas de relações de superioridade/inferioridade entre dominantes e dominados” (2005, p. 118).

estrutural e universal, o qual, para Quijano, configura uma das fundações da colonialidade que ainda hoje molda as relações de poder e conhecimento no mundo moderno.

A *colonialidade do poder* e o capitalismo mundial, portanto, coexistem e se reforçam mutuamente, operando como um sistema global de exploração e controle que articula raça, trabalho e capital em uma ordem hierárquica e desumanizadora. Quijano identifica, assim, que a dominação europeia e o desenvolvimento capitalista são inseparáveis da estrutura racial e colonial que originou e sustentou a modernidade, em um *padrão de poder* que define o capitalismo global e transcende o colonialismo tradicional, continuando a configurar as relações de trabalho e poder no mundo contemporâneo²¹². E essa é a razão pela qual Quijano aponta para a necessidade de reconhecer o colonialismo não apenas como uma fase histórica, mas como uma estrutura de poder que permanece ativa, subjacente ao capitalismo moderno, e que mantém populações racializadas em posições de desvantagem econômica e social.

A *colonialidade do poder* não se fundamenta, apenas, na dominação racial, mas também na centralidade da Europa Ocidental como sede do controle econômico e cultural do capitalismo mundial. A partir do século XVI, o tráfico comercial global intensificou-se com o fluxo de metais preciosos provenientes da América, promovendo um crescimento urbano acelerado e a expansão do mercado integrado e monetarizado na Europa Atlântica. Esse processo impulsionou a transformação da Europa Ocidental em uma nova identidade geocultural e em centro hegemônico do mercado mundial. O deslocamento do poderio econômico das costas do Mediterrâneo e da Ibéria para o Atlântico Norte-Occidental marca a formação de uma nova estrutura

²¹² Quijano observa que a centralidade europeia no controle do mercado mundial não decorre unicamente de fatores econômicos, mas também da maneira como a estrutura de trabalho não assalariado foi racializada e associada às populações colonizadas. Desde os primeiros momentos da colonização das Américas, as populações indígenas foram submetidas a formas extremas de exploração. Vistas como “raças inferiores”, essas populações foram sujeitas a um sistema de trabalho exaustivo e não remunerado, em que a força de trabalho era descartável, sendo os indígenas frequentemente forçados a trabalhar até a morte. A mortalidade não resultava apenas das doenças trazidas pelos colonizadores, mas, sobretudo, da exploração intensa e desumana imposta pelo sistema colonial. O genocídio dos povos indígenas nas primeiras décadas da colonização é, portanto, um reflexo da lógica de exploração racializada que fundamentava o sistema de trabalho colonial. (2005, p. 119).

global, na qual o eurocentrismo orienta a expansão do capitalismo e das relações de poder coloniais (Ibidem, p. 119).

A colonialidade e o capitalismo não são, desse modo, fenômenos isolados, mas partes de uma mesma matriz de poder que perpetua a exploração de populações racializadas²¹³. Essa estrutura global, que emergiu no contexto colonial, molda até hoje as relações entre Norte e Sul, centro e periferia, perpetuando uma ordem mundial onde as hierarquias raciais e a dominação econômica caminham lado a lado, garantindo a continuidade da exploração capitalista e colonial em novas formas e contextos.

Quijano também ressalta, com especial vigor, que não apenas em termos econômicos é que o capitalismo mundial, desde suas origens coloniais, é essencialmente eurocêntrico, mas também em sua visão cultural e epistemológica. A modernidade e a racionalidade foram construídas pelos europeus como produtos exclusivamente ocidentais, estabelecendo uma dicotomia em que a Europa se via como o centro da civilização, enquanto o resto do mundo era classificado como “primitivo” e “irracional”. Essa visão binária, expressa por categorias como Oriente-Occidente e primitivo-civilizado²¹⁴, sustentou a ideia de que a modernização de outras culturas era, em essência, uma europeização. Assim, a *colonialidade do poder* serviu como um instrumento para universalizar essa perspectiva eurocêntrica, configurando as relações culturais e intersubjetivas globais de maneira hierárquica.

²¹³ A lógica colonial do controle do trabalho foi essencial para a formação de uma nova estrutura global de exploração que estabeleceu uma “geografia social” do capitalismo. Sob essa estrutura, Quijano expõe como o trabalho assalariado era majoritariamente concentrado na Europa e entre os europeus, enquanto as formas de trabalho não remunerado – como a servidão e o trabalho forçado – foram atribuídas às populações colonizadas na América, África e Ásia. Essa divisão geográfica e racial do trabalho tornou-se central para o desenvolvimento capitalista, criando uma ordem de poder que colocava a Europa como centro econômico e cultural do mundo capitalista, reforçando o eurocentrismo.

²¹⁴ Algo já explorado no início do trabalho, com a referência à teoria dos sistemas mundiais e a menção aos chamados *core countries*, *peripheral countries*) e *semiperipheral countries*, em uma estrutura da qual os países centrais controlam e se beneficiam do mercado global. Nesse sentido, o próprio pensador peruano: “Quando Raúl Prebisch criou a célebre imagem de “Centro-Periferia” (The American Economic Review, 1959; ECLA, 1960; Baer, 1962), para descrever a configuração mundial do capitalismo depois da Segunda Guerra Mundial, apontou, sabendo-o ou sem saber, o núcleo principal do caráter histórico do padrão de controle do trabalho, de seus recursos e de seus produtos, que formava parte central do novo padrão mundial de poder constituído a partir da América. O capitalismo mundial foi, desde o início, colonial/moderno e eurocentrado. Sem relação clara com essas específicas características históricas do capitalismo, o próprio conceito de “moderno sistema-mundo” desenvolvido, principalmente, por Immanuel Wallerstein (1974-1989; Hopkins e Wallerstein, 1982) a partir de Prebisch e do conceito marxiano de capitalismo mundial, não poderia ser apropriada e plenamente entendido. QUIJANO, 2005, p. 120).

A constituição da América não apenas ampliou o mercado mundial, mas também alterou a forma como a humanidade percebia o tempo e a história. Com o surgimento de um sistema capitalista global, o conceito de futuro emergiu como um território temporal aberto e dinâmico, onde mudanças poderiam ser projetadas e moldadas pela ação humana. A ideia de um “futuro” tornou-se, assim, um elemento central da nova subjetividade moderna, diferenciando-se das concepções pré-modernas em que o tempo era visto como uma extensão do passado ou como algo determinado por forças divinas ou místicas. Essa transformação foi parte do que Quijano descreve como a “formação de uma nova intersubjetividade”, na qual o mundo passou a ser compreendido como um sistema global unificado pela colonialidade, pelo capitalismo e pelo eurocentrismo²¹⁵.

Esse *eurocentrismo*, formado a partir do século XVII, consolidou-se como uma visão de mundo que interpreta o desenvolvimento histórico e social dos povos não europeus como uma prévia do estado “civilizado” europeu. Estruturado em torno da lógica burguesa e das necessidades do capitalismo global, o eurocentrismo define-se por um entendimento evolucionista e dualista da história humana, em que o desenvolvimento ocidental é visto como o ápice da civilização.

Para o eurocentrismo, as diversas formas de organização do trabalho — reciprocidade, escravidão, servidão e produção mercantil independente — são entendidas como estágios pré-capitalistas, posicionados em uma linha evolutiva que culmina na mercantilização da força de trabalho. Essa visão não apenas desconsidera a diversidade das formas de trabalho, mas as interpreta como incompatíveis com o capital, um entendimento que não reflete a realidade colonial. Na América, todas essas formas de controle do trabalho foram deliberadamente organizadas e adaptadas para atender às necessidades do capitalismo emergente, formando um sistema em que a exploração dos povos colonizados fornecia a base para a acumulação de capital e o desenvolvimento do mercado mundial. O eurocentrismo, ao não reconhecer essa integração, apresenta uma narrativa unilateral e distorcida,

²¹⁵ Novamente, nas palavras de QUIJANO: “Todo esse acidentado processo implicou no longo prazo uma colonização das perspectivas cognitivas, dos modos de produzir ou outorgar sentido aos resultados da experiência material ou intersubjetiva, do imaginário, do universo de relações intersubjetivas do mundo; em suma, da cultura”. (2005, p. 121).

ocultando a complexidade do sistema colonial/moderno e a maneira como ele integra diferentes modos de trabalho sob o domínio do capital.

O eurocentrismo criou, portanto, uma perspectiva dualista que divide o mundo entre civilizado e primitivo, moderno e tradicional, científico e mágico/mítico. Esse dualismo naturalizou a supremacia europeia e relegou as culturas não europeias a uma posição de "primitivismo", classificando-as como etapas anteriores na trajetória de desenvolvimento humano. Esse processo, embasado em uma visão racializada, reduziu a rica diversidade cultural dos povos indígenas da América e dos africanos a categorias homogêneas e negativas, como "índios" e "negros", despojando-os de suas identidades históricas. Essa identidade racial colonial e negativa implicava, por sua vez, a exclusão desses povos da "história da produção cultural da humanidade", confinando-os a uma posição de inferioridade permanente²¹⁶.

O eurocentrismo articula, diante de todo esse cenário, uma estrutura de poder em que o capitalismo é legitimado por meio de uma narrativa histórica em que o Ocidente representa a vanguarda da humanidade. Para os europeus, a modernidade e a racionalidade foram imaginadas como criações exclusivamente ocidentais, relegando os povos não europeus a uma condição de atraso. Essa perspectiva evolucionista e etnocêntrica, baseada em mitos de progresso e civilização, justifica a exploração colonial e a hierarquia racial. A narrativa eurocêntrica da modernidade, ao conceber os europeus como autossuficientes e autogerados, ignora que a própria constituição da Europa como entidade geocultural moderna e centro do capitalismo mundial dependeu do trabalho não remunerado e das riquezas extraídas das colônias americanas e africanas.

O modelo eurocêntrico da modernidade capitalista foi, assim, decisivo para as desigualdades globais que se acentuaram após a independência política das colônias. Embora muitos países da América Latina e outros locais tenham se tornado

²¹⁶ A perspectiva eurocêntrica de conhecimento opera, segundo Aníbal Quijano, como um "espelho distorcido" para a América Latina, refletindo a realidade da região de maneira parcial e incompleta. Embora a América Latina possua importantes traços europeus, que se manifestam tanto material quanto intersubjetivamente, sua realidade social e histórica permanece profundamente distinta. Esse espelho eurocêntrico condiciona a população latino-americana a enxergar-se através de uma lente estrangeira, aceitando uma imagem de si mesma que não corresponde inteiramente à sua identidade. Como consequência, essa visão distorcida impede uma compreensão plena e autônoma dos desafios enfrentados pela região, conduzindo-a a soluções incompletas e distorcidas para seus problemas sociais e políticos. (2005, p. 122).

formalmente independentes, a economia e a sociedade nesses territórios continuaram subordinadas aos interesses e valores coloniais, perpetuando uma dominação que mantinha essas regiões como periferias do sistema capitalista global. A independência política, ao invés de promover uma verdadeira emancipação, frequentemente reforçou as estruturas coloniais, convertendo as ex-colônias em economias dependentes e mantendo o caráter colonial do capitalismo global. Além disso, o humanista peruano nos ensina que, para o capitalismo, o mercado não só estabelece os limites da possível igualdade social, mas também define os meios e fins do processo de modernização. Nesse sentido, o liberalismo europeu – que enfatiza a igualdade formal no mercado – é uma expressão das condições materiais e subjetivas que moldaram a sociedade ocidental, enquanto, para o restante do mundo, o controle do trabalho ainda se fundamenta majoritariamente em formas não salariais, mantendo uma estrutura colonial de dominação, mesmo em nações politicamente independentes.

O eurocentrismo é, em síntese, uma ferramenta intelectual da colonialidade do poder, um sistema de dominação que não apenas controla os recursos e o trabalho, mas também define quem possui legitimidade no campo do conhecimento. A experiência histórica da América e da Europa demonstra que o capitalismo mundial é, fundamentalmente, uma estrutura heterogênea, onde diferentes formas de controle do trabalho e diversas identidades raciais e culturais são subordinadas ao capital²¹⁷. Esse sistema, constituído em torno da América, não só explora economicamente os povos colonizados, mas também desumaniza e desvaloriza suas culturas, impondo o padrão europeu como o único caminho para a civilização.

Outro conceito, gerado no âmbito do eurocentrismo e que impactou na conformação da *colonialidade do poder*, é o de *Estado-Nação*. Com efeito, tal conceito foi estabelecido, no âmbito da modernidade, como modelo político por excelência, mas sua aplicação na América Latina revela as limitações e contradições desse ideal.

²¹⁷ A partir da colonialidade do poder, o capitalismo tornou-se um sistema heterogêneo que articula diversas formas de controle do trabalho em uma estrutura interdependente e conflitiva, onde a exploração econômica e a dominação cultural caminham lado a lado. As necessidades do capital impulsionaram a formação de um sistema-mundo onde o eurocentrismo atua como uma lógica central de controle, impondo-se como uma perspectiva de conhecimento que legitima e perpetua a estrutura de desigualdade global. Quijano enfatiza, com base nisso, que essa visão distorcida da história humana foi crucial para a hegemonia global do eurocentrismo e a expansão do capitalismo mundial.

Na Europa, o processo de formação do Estado-nação, ensina Quijano, envolveu uma integração social progressiva, com ampliação da participação democrática e um processo gradual de colonização interna que homogeneizou populações diversas. Esse processo de nacionalização incluiu, por exemplo, a expulsão de grupos “estrangeiros” indesejados, como judeus e muçulmanos na Espanha, mas, em geral, permitiu a democratização parcial e a criação de uma identidade nacional. A experiência europeia de formação do Estado-nação é marcada, portanto, por um relativo sucesso na integração política e social das populações e pelo estabelecimento de estruturas de poder centralizadas que promoviam uma identidade nacional unificada (QUIJANO, p. 130).

Na América Latina, por outro lado, a criação de Estados-nação modernos foi fundamentada na perspectiva eurocêntrica²¹⁸, mas enfrentou obstáculos substanciais devido à diversidade étnica e à persistência de relações coloniais internas. Em vez de promover uma verdadeira descolonização das relações sociais e políticas, os Estados latino-americanos seguiram um caminho de exclusão e violência contra as populações indígenas, negras e mestiças. No Sul global, por exemplo, a homogeneização social foi alcançada principalmente por meio da eliminação massiva de indígenas e afrodescendentes, em um esforço para criar uma identidade nacional branca que se aproximasse do modelo europeu. Esse processo de exclusão, e não de integração democrática, deixou os Estados latino-americanos vulneráveis a instabilidades políticas e a crises de identidade²¹⁹.

²¹⁸ Quijano leciona que “por outro lado, o processo de centralização estatal que antecedeu na Europa Ocidental a formação de Estados-nação, foi paralelo à imposição da dominação colonial que começou com a América. Quer dizer, simultaneamente com a formação dos impérios coloniais desses primeiros Estados centrais europeus. O processo tem, pois, um duplo movimento histórico. Começou como uma colonização interna de povos com identidades diferentes, mas que habitavam os mesmos territórios transformados em espaços de dominação interna, ou seja, nos próprios territórios dos futuros Estados-nação. E continuou paralelamente à colonização imperial ou externa de povos que não só tinham identidades diferentes das dos colonizadores, mas que habitavam territórios que não eram considerados como os espaços de dominação interna dos colonizadores, quer dizer, não eram os mesmos territórios dos futuros Estados-nação dos colonizadores”. (2005, p. 131).

²¹⁹ O caso do Brasil destaca-se pela forte presença de uma população negra escravizada, que era essencial para a economia colonial e, mais tarde, para a economia do novo Estado-nação. Os negros e a maioria dos indígenas, especialmente aqueles da Amazônia, foram considerados “estrangeiros” dentro do próprio território, mantendo-se à margem do projeto nacional. Esse processo, marcado por relações coloniais e raciais desiguais, dificultou a construção de um Estado-nação que verdadeiramente representasse a diversidade da população brasileira.

A aplicação do conceito de Estado-nação moderno na América Latina, assim, revela uma contradição fundamental: enquanto os Estados europeus alcançaram um certo grau de integração social e democracia, os Estados latino-americanos, formados sob a lógica eurocêntrica, impositiva de uma visão idealizada e distorcida do Estado-nação, tiveram obscurecidas suas possibilidades de uma verdadeira emancipação, e mantiveram estruturas de dominação colonial. Os movimentos de independência das colônias ibéricas foram liderados por elites que buscavam autonomia política sem, contudo, realizar uma verdadeira descolonização social e econômica. Essa resistência à transformação social e à inclusão das populações indígenas e negras perpetuou as desigualdades e manteve a estrutura colonial dentro dos Estados formalmente independentes da América Latina.

Por fim, Aníbal Quijano explora o conceito de *dependência histórico-estrutural*, para descrever a complexa relação entre as elites brancas dos Estados latino-americanos independentes e as potências capitalistas europeias. Diferentemente de uma dependência econômica ou política convencional, os dominadores latino-americanos, ao consolidarem sua posição social, mantinham interesses explícitos e antagônicos em relação à maioria da população – composta por índios, negros e mestiços – que constituía a base trabalhadora da sociedade. Esses interesses estavam mais alinhados aos dos europeus do que aos das populações locais, revelando uma comunidade de interesses raciais que distanciava as elites dos problemas e demandas nacionais. A colonialidade do poder perpetuava uma lógica de dominação que impedia a consolidação de um interesse nacional comum, alimentando uma condição de dependência não por subordinação econômica a outra potência, mas por uma afinidade cultural e ideológica com os europeus²²⁰.

²²⁰ O esforço teórico de Quijano vai ao encontro da contundência de Darcy Ribeiro. O antropólogo brasileiro afirma que: “No Brasil, de índios e negros, a obra colonial de Portugal foi também radical. Seu produto verdadeiro não foram os ouros afanosamente buscados e achados, nem as mercadorias produzidas e exportadas. Nem mesmo o que tantas riquezas permitiram erguer no Velho Mundo. Seu produto real foi um povo-nação, aqui plasmado principalmente pela mestiçagem, que se multiplica prodigiosamente como uma morena humanidade em flor, à espera do seu destino. Claro destino, singelo, de simplesmente ser, entre os povos, e de existir para si mesmos. Nada é mais continuado, tampouco é tão permanente, ao longo desses cinco séculos, do que essa classe dirigente exógena e infiel a seu povo. No afã de gastar gentes e matas, bichos e coisas para lucrar, acabam com as florestas mais portentosas da terra. Desmontam morrarias incomensuráveis, na busca de minerais. Erodem e arrasam terras sem conta. Gastam gente, aos milhões. Tudo, nos séculos, transformou-se incessantemente. Só ela, a classe dirigente, permaneceu igual a si mesma, exercendo sua interminável hegemonia. Senhorios velhos se sucedem em senhorios novos, super-homogêneos e solidários entre si, numa férrea união superarmada e a tudo predisposta para manter o povo gemendo e produzindo.

Essa dependência levou as elites latino-americanas a resistirem a mudanças sociais que ameaçassem sua posição de dominadores. O capital acumulado nas colônias era direcionado ao consumo ostentoso de bens europeus, em vez de investir na criação de um mercado interno e na industrialização local. A formação de um capital industrial independente, que exigiria a transformação dos trabalhadores servos e escravos em assalariados, não interessava a essa elite. Quando, mais tarde, a abolição da escravidão tornou-se inevitável, a resposta foi a substituição dos trabalhadores negros e indígenas por imigrantes europeus, ao invés de promover a inclusão e assalariamento dos libertos.

A dependência histórico-estrutural e a persistência da colonialidade do poder refletem-se, portanto, na dificuldade de se construir uma cidadania inclusiva e um Estado-nação moderno na América Latina. A perspectiva eurocêntrica, ao impor modelos inadequados, obscurece a realidade e limita as possibilidades de transformação social. A solução, segundo Quijano, passa pela superação desse “espelho eurocêntrico” e pela busca de uma identidade e de um projeto político próprios, que reconheçam a diversidade racial e cultural da América Latina e promovam uma verdadeira democratização e descolonização das relações de poder. Somente com a desconstrução da colonialidade do poder será possível avançar rumo a uma América Latina que seja verdadeiramente independente, democrática e inclusiva.

Abordar, com a profundidade apresentada, os aspectos que caracterizam o conceito de *colonialidade do poder*, se torna tarefa inafastável na busca por uma compreensão teórica responsável acerca do fenômeno que diversos países periféricos – e, especialmente, para o presente trabalho, o Brasil – experimentam mediante a exploração política, econômica e cultural massiva dos dados pessoais produzidos por seus cidadãos. Em verdade, os estudos sobre a colonialidade são fundamentais para entender o Brasil contemporâneo, pois revelam como as estruturas de poder e hierarquias herdadas do colonialismo continuam a influenciar as relações econômicas, sociais e culturais no país. No contexto brasileiro, marcado pela

Não o que querem e precisam, mas o que lhes mandam produzir, na forma que impõem, indiferentes a seu destino. Não alcançam, aqui, nem mesmo a façanha menor de gerar uma prosperidade generalizável à massa trabalhadora, tal como se conseguiu, sob os mesmos regimes, em outras áreas. Menos êxito teve, ainda, em seus esforços por integrar-se na civilização industrial. Hoje, seu desígnio é forçar-nos à marginalidade na civilização que está emergindo. (RIBEIRO, 2015, p. 53).

desigualdade racial e social, o conceito de *colonialidade do poder* de Aníbal Quijano é uma ferramenta essencial para compreender como a história colonial moldou e ainda molda a estrutura de classes e as oportunidades econômicas, reforçando uma hierarquia racial que marginaliza grande parte da população. Essa perspectiva permite enxergar a persistência de um modelo de dominação e exploração enraizado no colonialismo, o qual impacta diretamente a distribuição de recursos e o acesso a direitos, particularmente para os grupos racializados e socialmente vulneráveis.

Em razão disso, não é excessivo repisar que a construção do conceito de *colonialidade do poder* por Aníbal Quijano abrange diversas dimensões que compõem a matriz de dominação e exploração herdada do colonialismo e adaptada ao capitalismo global. Primeiramente, o *controle do trabalho* envolve a subordinação de diferentes formas de trabalho (servil, escravo, assalariado) ao capital, estabelecendo um padrão global de exploração que integra todos os modos de produção ao mercado mundial. Em segundo lugar, o *controle da sexualidade e do gênero* se manifesta na imposição de normas e valores eurocêntricos, subordinando a diversidade de práticas e relações afetivas e reprodutivas aos padrões do patriarcado ocidental. O terceiro eixo é o *controle da subjetividade e do conhecimento*, pelo qual a colonialidade define uma hierarquia epistêmica que privilegia o conhecimento ocidental e marginaliza ou deslegitima os saberes indígenas e africanos, estabelecendo o eurocentrismo como base de uma racionalidade que se pretende universal. Por fim, o *controle da autoridade política* sustenta a hegemonia das potências coloniais, mesmo após a independência formal das colônias, ao influenciar a organização dos Estados nacionais e o funcionamento das instituições, perpetuando as hierarquias estabelecidas pelo colonialismo. Esses quatro eixos — trabalho, sexualidade e gênero, subjetividade e conhecimento, e autoridade política — articulam-se para constituir um sistema global assentado sobre o que Quijano denominou como "colonialidade do poder".

Além dos eixos de dominação descritos, com caracterização mais ampla e genérica, a colonialidade do poder de Quijano é sustentada por conceitos adicionais que aprofundam a compreensão de como o colonialismo moldou as estruturas globais e perpetua a exploração e a subordinação. O *controle, exploração e divisão do trabalho* são centrais, pois estabeleceram uma hierarquia de atividades econômicas

associadas a identidades racializadas, vinculando trabalhos manuais e exploratórios aos povos colonizados e reservando atividades administrativas e de controle aos colonizadores. A *classificação racial da humanidade* reforça essa divisão, criando uma estrutura onde a "raça" funciona como marcador para a distribuição de papéis sociais e econômicos, legitimando a subordinação de grupos não europeus com base em uma suposta inferioridade natural. O *eurocentrismo* consolida essa hierarquia ao apresentar a cultura e o conhecimento europeus como universais, marginalizando e desvalorizando as culturas e saberes dos povos colonizados, e construindo a modernidade como um projeto exclusivamente ocidental.

Outro conceito-chave é o do *Estado-nação*, uma forma de organização política difundida pelo colonialismo e adaptada ao contexto latino-americano de maneira a reforçar a exclusão das populações indígenas e afrodescendentes, promovendo uma homogeneização cultural que silencia as diversidades locais. Finalmente, a *dependência histórico-estrutural* se refere ao alinhamento das elites latino-americanas com os interesses das potências coloniais e do capital europeu, impedindo uma verdadeira emancipação econômica e social ao manter as ex-colônias em um estado de subordinação ao mercado e cultura globais. Esses conceitos, interligados, formam uma matriz de poder que continua a influenciar as relações econômicas, políticas e culturais, perpetuando desigualdades e impondo o modelo colonial como norma para as sociedades do Sul Global.

E é a partir dessa compreensão profunda sobre a *colonialidade* que o conceito de *colonialismo de dados* se apresenta como uma extensão contemporânea dessas práticas, agora aplicada ao controle e à exploração de dados pessoais. Teóricos como Nick Couldry e Ulises A. Mejias argumentam que a extração e apropriação de dados representa um novo tipo de colonialismo, em que a própria vida humana é convertida em recurso econômico, reproduzindo a lógica de dominação da colonialidade. Essa prática de "colonização digital" dialoga diretamente com as ideias de Quijano, pois, assim como no passado o corpo e o trabalho dos povos colonizados eram explorados para sustentar o capital, hoje são as informações pessoais e as interações diárias que se tornam fontes de valor.

Nick Couldry e Ulises A. Mejias são estudiosos que exploram o impacto do capitalismo de dados e suas implicações sociais e políticas. Nick Couldry²²¹, professor de Mídia, Comunicações e Teoria Social na *London School of Economics*, é conhecido por suas contribuições críticas sobre o poder midiático, práticas de representação e teorias de mídia e sociedade. Ulises A. Mejias²²², professor na Universidade Estadual de Nova York em Oswego, se dedica ao estudo da comunicação crítica e ao papel da tecnologia na perpetuação de desigualdades. Juntos, assinam escritos como *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (2019, Stanford University Press), e *Data Grab: The New Colonialism of Big Tech and How to Fight Back* (2024, Penguin Random House and University of Chicago Press). No âmbito desses escritos, examinam justamente como o colonialismo de dados transforma relações humanas em dados para apropriação capitalista, alertando sobre os efeitos de práticas extrativas digitais que comprometem a soberania e a dignidade dos indivíduos e comunidades.

Em *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (2019, Stanford University Press), Couldry e Mejias argumentam que a relação de extração e apropriação de dados configura uma nova forma de colonialismo, que denominam, justamente, como *colonialismo de dados*. Esse conceito representa a extensão contemporânea de práticas coloniais que envolvem a apropriação da vida humana, agora sob a forma de dados, visando à geração de valor econômico. Tal prática não se limita a capturar o trabalho ou a produção de bens materiais, mas abrange a própria vida humana em seus detalhes mais cotidianos, transformando interações sociais e atividades triviais em insumos apropriados para o capital (COULDRY; MEJIAS, 2019, p. 9-10).

O conceito de *colonialismo de dados* se fundamenta na analogia entre os processos históricos de colonialismo territorial e a apropriação contemporânea de dados. Assim como no passado, quando terras e corpos foram subjugados para exploração econômica, o colonialismo de dados, de acordo com Couldry e Mejias, em *Data Grab: The New Colonialism of Big Tech and How to Fight Back* (2024, Penguin

²²¹ Para um perfil completo de Nick Couldry, ver: <https://www.lse.ac.uk/media-and-communications/people/academic-staff/nick-couldry>. Acesso em: 14 mar. 2024.

²²² Para um perfil completo de Ulises A. Mejias, ver: <https://ww1.oswego.edu/communication-studies/profile/ulises-mejias>. Acesso em: 14 mar. 2024.

Random House and University of Chicago Press), busca capturar a experiência humana, convertendo-a em um recurso ininterrupto de valor. Esse processo é realizado por meio do que os autores denominam como "*data grab*" (apropriação de dados) em larga escala, semelhante ao que foi historicamente visto com a exploração de territórios e populações colonizadas (COULDRY; MEJIAS, 2024, p. 8). Uma vez apropriados, esses dados tornam-se elementos centrais das chamadas "relações de dados" (*data relations*), que reconfiguram a vida social ao naturalizar a extração de dados como uma prática comum e aparentemente inofensiva. Essa dinâmica resulta na erosão da autonomia humana, pois a existência cotidiana passa a ser continuamente monitorada e manipulada para atender aos interesses do capital, transformando a vigilância em uma condição intrínseca da vida moderna (COULDRY; MEJIAS, 2019, p. 16-18).

O conceito de colonialismo de dados dialoga diretamente com as teorias da *colonialidade do poder* de Aníbal Quijano. O sociólogo peruano argumenta que a colonialidade não é apenas um fenômeno histórico, mas um padrão de poder que persiste e molda as relações sociais e econômicas no mundo contemporâneo. Couldry e Mejias descrevem, a partir de Quijano e consoante aprofundado alhures, a colonialidade como um processo que impõe uma hierarquia global baseada em raça e conhecimento, perpetuando a exploração e a dominação dos povos e culturas considerados inferiores, especialmente os do Sul Global (COULDRY; MEJIAS, 2019, p. 22).

Inspirados por essa abordagem, Couldry e Mejias veem o colonialismo de dados como uma continuação da lógica colonial em que, ao invés da exploração de territórios físicos, é a própria vida humana que é colonizada pela infraestrutura digital e pelas práticas de extração de dados. Eles argumentam que a lógica de apropriação do colonialismo histórico foi adaptada para o contexto atual, onde a extração de dados se torna central para a acumulação de capital. Assim, a colonialidade do poder se manifesta na forma de colonialismo de dados, mantendo a estrutura de dominação e de exploração através da tecnologia e do capital global (COULDRY; MEJIAS, 2019, p. 30-31), bem como mediante a reorganização das relações sociais e culturais, impondo modos de ser, saber e sentir dos colonizadores sobre os colonizados. Defendem, desse modo, que o colonialismo de dados reflete essa mesma

"colonialidade", pois ao controlar os fluxos de dados e definir narrativas e percepções da realidade, as grandes corporações tecnológicas estão efetivamente moldando a subjetividade e a identidade cultural contemporâneas, impondo uma versão moderna de "domínio" cultural e ideológico (COULDRY; MEJIAS, 2024, p. 47).

Vê-se, portanto, que um dos elementos centrais para a compreensão do pensamento do sociólogo inglês e do pensador mexicano é a compreensão de que o "colonialismo de dados" não se restringe a um mero uso tecnológico, mas reflete uma imposição estrutural, onde a coleta e processamento de dados (informações das atividades e relações humanas) são realizados sem consentimento total ou entendimento das populações sobre as consequências dessa coleta. Para Mejias e Couldry, essa coleta indiscriminada é, repise-se, uma atualização da lógica colonial de exploração, transformando vidas e experiências em ativos que podem ser comercializados, assim como aconteceu no passado com as terras e riquezas naturais (COULDRY; MEJIAS, 2024, p. 15-22).

Uma análise mais minuciosa do conceito de colonialismo de dados passa pelo que Couldry e Mejias definem como os "quatro X's do colonialismo" – explorar, expandir, extrair e exterminar – etapas historicamente aplicadas ao colonialismo clássico que, na contemporaneidade, sustentam a extração massiva de dados pessoais. O primeiro "X", explorar, manifesta-se na busca incessante das plataformas digitais em penetrar cada aspecto da vida privada, capturando informações pessoais, comportamentais e contextuais. Esse processo é essencial para transformar a experiência cotidiana em "territórios de dados", permitindo uma vigilância minuciosa que converte todos os aspectos da vida humana em elementos mensuráveis e monetizáveis. A seguir, ocorre a expansão, na qual essas práticas de coleta e monitoramento extrapolam fronteiras, envolvendo cada vez mais domínios da vida pública e privada, ao ponto de algoritmos serem integrados de forma imperceptível em atividades triviais, normalizando uma relação dependente e extrativa entre usuário e tecnologia.

O terceiro "X", extrair, relaciona-se à apropriação e monetização direta dessas informações, que deixam de ser simples dados brutos e se transformam em produtos e insights de mercado altamente lucrativos. Aqui, as plataformas não apenas capitalizam essas informações, mas reconfiguram a economia digital para sustentar

esse ciclo extrativo, colocando o comportamento humano a serviço de uma lógica ininterrupta de acumulação de capital. Finalmente, o processo culmina no extermínio, onde a diversidade cultural e as práticas autônomas são sistematicamente sufocadas. A imposição de padrões globais de consumo e controle, mediados por algoritmos e orientados por interesses corporativos, resulta na homogeneização cultural e na eliminação de alternativas independentes, apagando modos de vida locais e estruturas econômicas que não se alinham aos interesses das plataformas digitais. Dessa forma, os “quatro X's” revelam como o colonialismo de dados não apenas reproduz, mas adapta e expande a lógica colonialista tradicional, subordinando a autonomia humana aos imperativos de um capitalismo global e digitalizado (COULDRY; MEJIAS, 2024, p. 28-35).

No cenário brasileiro dos estudos sobre a proteção de dados pessoais, destaca-se a influência de Quijano, Couldry e Mejias na obra *Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal* (2021), organizada por João Francisco Cassino, Joyce Souza e Sérgio Amadeu da Silveira. Em referido livro, cujos capítulos contam com a autoria de pesquisadoras e pesquisadores do Doutorado e do Mestrado do Programa de Pós-Graduação em Ciências Humanas e Sociais da Universidade Federal do ABC (UFABC), integrantes do Laboratório de Tecnologias Livres (LabLivre/UFABC), localizado em São Bernardo do Campo-SP, e sob a coordenação do professor Sérgio Amadeu da Silveira, são discutidas as nuances e complexidades do colonialismo de dados como um processo de expropriação digital alinhado aos interesses do neoliberalismo, com especial atenção ao posicionamento do Brasil nesse contexto.

Em *o Sul Global e os desafios pós-coloniais na era digital*, João Francisco Cassino promove uma análise sobre o “colonialismo de dados”, explorando as nuances fornecidas por Nick Couldry e Ulises A. Mejias. Esse conceito, conforme Cassino, desnuda o surgimento de uma nova forma de dependência tecnológica e de poder, já que se refere ao processo de apropriação da vida social e da subjetividade humana para fins de acumulação capitalista, replicando as dinâmicas extrativas e predatórias do colonialismo histórico. Conforme apontado por Couldry e Mejias, o uso do termo “colonialismo” não é meramente metafórico, mas se baseia na continuidade das práticas coloniais de apropriação e controle que agora são adaptadas ao âmbito

digital, utilizando métodos computacionais de quantificação abstrata para reconfigurar as relações de poder globais (CASSINO; SILVEIRA; SOUZA, 2021, p. 15).

No contexto do colonialismo de dados, a quantificação da vida social em plataformas digitais permite que dados pessoais sejam coletados, transformados em perfis e posteriormente utilizados para formatar o comportamento dos indivíduos. Esse processo é descrito como uma nova etapa de exploração onde o capital não precisa mais de fronteiras físicas para extrair recursos, mas sim de uma infraestrutura digital que captura e armazena dados de maneira constante e abrangente (CASSINO; SILVEIRA; SOUZA, 2021, p. 16). Dessa forma, as relações sociais tornam-se elementos passíveis de serem extraídos e monetizados, fazendo com que os sujeitos colonizados, no sentido digital, se vejam constantemente categorizados e julgados com base nos próprios dados que fornecem, muitas vezes sem qualquer clareza sobre como essas informações são utilizadas.

Cassino também menciona a ideia de “relações baseadas em dados” de Couldry e Mejias, que denota um tipo de relação social moldada pela extração e exploração de informações pessoais em massa. Em sua análise, essas “relações de dados” representam uma transformação radical das interações humanas, onde cada aspecto da vida social é convertido em dado e, por conseguinte, explorado pelo mercado global (CASSINO; SILVEIRA; SOUZA, 2021, p. 17). Em um cenário onde o Brasil e outras nações do Sul Global frequentemente estão sujeitas à coleta massiva de dados por empresas do Norte Global, o colonialismo de dados reflete a contínua desigualdade de poder e recursos entre essas regiões. As práticas de empresas de tecnologia, em particular, revelam a dependência digital criada pela influência dessas corporações nas políticas locais e mercados, intensificando uma nova forma de dependência que replica a lógica colonial histórica.

Além disso, Cassino destaca como a opacidade do processo de coleta e análise de dados afeta os indivíduos, que muitas vezes não têm ciência de quais informações são coletadas nem de como elas são empregadas. Essa assimetria informacional é uma característica fundamental do colonialismo de dados, pois impede que as populações compreendam o impacto de suas interações digitais, transformando-as em sujeitos colonizados que vivem sob o constante rastreamento e categorização (CASSINO; SILVEIRA; SOUZA, 2021, p. 18). Em última análise, essa dinâmica reflete

o caráter invasivo das práticas de coleta de dados, onde o monitoramento de informações pessoais se torna um aspecto inescapável da vida contemporânea, levando a uma modulação algorítmica dos comportamentos individuais e sociais.

Cassino também propõe uma reflexão a partir das observações de Shoshana Zuboff sobre o “capitalismo de vigilância”, que pode ser complementada pelas ideias de Coudry e Mejias. Esse conceito destaca como as grandes empresas de tecnologia não apenas capturam e processam dados em massa, mas também utilizam essas informações para influenciar e controlar o comportamento dos usuários, criando novos mercados e oportunidades de lucro a partir da previsão e modulação de práticas sociais e de consumo (CASSINO; SILVEIRA; SOUZA, 2021, p. 19). Em consonância com o colonialismo de dados, o capitalismo de vigilância – particularmente nas regiões do Sul Global, onde o acesso desigual à tecnologia e à infraestrutura digital amplifica a vulnerabilidade das populações locais às dinâmicas extrativas digitais – evidencia a transformação da vida social em um recurso altamente lucrativo, onde o valor é gerado não pela produção de bens tangíveis, mas pelo controle das informações e das interações humanas, em uma formatação que se assemelha às relações coloniais, já que a exploração dos dados pessoais e a falta de controle sobre seu uso colocam os indivíduos periféricos em uma posição de dependência, à exemplo de outrora, quando onde os recursos eram extraídos e beneficiavam exclusivamente as potências colonizadoras²²³.

Por sua vez, Sérgio Amadeu da Silveira, em *A hipótese do colonialismo de dados e o neoliberalismo*, enriquece o debate sobre o tema ao apresentar uma compreensão mais ampla sobre a permanência da colonialidade como fundamento do capitalismo global. Para Amadeu – em manifesto endosso aos ensinamentos de

²²³ Shoshana Zuboff é renomada filósofa e autora, é amplamente reconhecida por desenvolver o conceito de “capitalismo de vigilância”, abordado em sua obra “A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder” (2020). Zuboff descreve esse modelo econômico como uma nova lógica capitalista que explora a vida digital por meio da coleta massiva de dados, sem o consentimento dos usuários, para prever e influenciar comportamentos, gerando enormes lucros. Suas ideias convergem com a análise sobre o colonialismo de dados, uma vez que ambas as abordagens denunciam a transformação de dados pessoais em recursos econômicos explorados de maneira unilateral, com especial impacto em regiões do Sul Global. Em ambos os casos, os indivíduos têm suas informações coletadas e processadas de forma que os coloca em posição de desvantagem e dependência, semelhante à exploração colonial, onde o benefício econômico é direcionado a grandes corporações ou potências hegemônicas, enquanto a autonomia e o controle dos dados são negados aos seus verdadeiros donos. No presente trabalho, adotou-se, em profundidade, as análises sobre o assunto a partir de Carissa Véliz e de Zygmunt Bauman, razão pela qual não se verticalizou o tema a partir de Zuboff.

Quijano – a colonialidade transcende o colonialismo histórico e persiste como um sistema de poder que hierarquiza epistemologias, modos de vida e culturas, relegando as comunidades não-ocidentais a uma condição de sujeição e subordinação. Nesse sentido, afirma que a colonialidade é intrínseca ao neoliberalismo contemporâneo, pois ambos operam por meio da desvalorização de saberes locais e da imposição de modelos de pensamento alinhados aos interesses econômicos dominantes (CASSINO; SILVEIRA; SOUZA, 2021, p. 37).

Para contextualizar a relação entre neoliberalismo e colonialidade, Amadeu recorre às obras, *v.g.* de Dardot e Laval, de David Harvey e de Wendy Brown, entre outros, evidenciando que o neoliberalismo reorganiza a vida social ao colocar o mercado no centro de todas as dimensões da existência humana²²⁴. Esse arranjo resulta na construção de um sistema em que as grandes corporações de tecnologia, ou "*big techs*", controlam as interações humanas por meio de plataformas de dados, modulando comportamentos e influenciando decisões. O neoliberalismo, assim, atua como uma extensão da colonialidade ao intensificar a dependência dos países periféricos em relação às tecnologias desenvolvidas no Norte Global, ampliando a desigualdade e subjugando as populações locais aos interesses das corporações (CASSINO; SILVEIRA; SOUZA, 2021, p. 42).

²²⁴ Sérgio Amadeu da Silveira: "Laval e Dardot, inspirados em Foucault, detectaram que o neoliberalismo é a forma atual de nossa existência e que se impõe como o ordenamento do capitalismo contemporâneo. Alicerçados no marxismo, David Harvey, Gérard Duménil e Dominique Lévy consideraram a neoliberalização como a dinâmica geral do capital que opera em benefício das camadas mais altas de renda, resultante do compromisso entre as classes capitalistas e a camada superior da classe gerencial, sob a hegemonia financeira. Wendy Brown observou que o neoliberalismo coloca a legitimidade do Estado subordinada à capacidade de servir a racionalidade econômica, solapando o vínculo entre capitalismo e democracia, subordinando tudo, principalmente a lógica do Estado, às empresas e à sua rentabilidade. Pesquisadores de inspirações tanto marxista quanto foucaultiana identificam que o neoliberal desloca a empresa para o centro de gravidade da existência e faz do Estado seu maior serviçal. Nesse sentido, as relações contratuais entre capital e trabalho se tornam relações entre empresas de variados tamanhos, inclusive, empresas de um único funcionário, que é o seu próprio dono. A dinâmica neoliberal reforça a colonialidade. Primeiro, a boa cartilha neoliberal manda que as empresas privadas assumam todas as atividades econômicas. Assim, cabe ao Estado assegurar que essas empresas assumam a criação, execução e manutenção do máximo de ações possíveis. Segundo, o *ethos* da concorrência manda apostar no menor preço com a melhor qualidade – esta nem sempre exigida. Terceiro, o desenvolvimento virá da escolha e do consumo dos melhores produtos e serviços, independentemente de outros valores ou princípios, como local de produção e benefícios sociais. Assim, para o neoliberal não seria sustentável a opção de criar e manter serviços executados pelo Estado, nem gastar recursos que deveriam ser investidos em empresas privadas, muito menos tentar soluções custosas de desenvolver localmente o que pode ser obtido globalmente. O neoliberalismo utiliza com anabolizantes a teoria das vantagens comparativas de David Ricardo". (CASSINO; SILVEIRA; SOUZA, 2021, p. 38-39).

No âmbito do capitalismo digital, a *dataficação* – ou transformação da vida social em dados – tornou-se uma prática central do neoliberalismo contemporâneo. Amadeu argumenta que, com a expansão da economia digital, a coleta e monetização de dados pessoais passaram a constituir um mercado de grande valor, onde empresas como Google e Facebook acumulam um poder econômico sem precedentes. No entanto, essa dinâmica extrativa reforça a colonialidade de dados, pois os fluxos de informações vão dos países periféricos para os grandes centros tecnológicos, que detêm o monopólio das tecnologias e do conhecimento algorítmico²²⁵. Como resultado, a dependência tecnológica e econômica dos países periféricos se intensifica, estabelecendo, justamente, um novo tipo de relação colonial.

Amadeu aponta, por fim, para a necessidade de resistir à colonialidade de dados por meio de pesquisas que exponham as estruturas de poder que sustentam esse sistema – justamente um dos objetivos que alicerçam a presente tese. Argumenta que a superação das assimetrias geradas pelo colonialismo de dados depende da criação de tecnologias que promovam a inteligência coletiva e a soberania digital dos países do Sul Global. Para tanto, Amadeu defende que a reforma das práticas de gestão pública deve priorizar a independência digital e o desenvolvimento de soluções tecnológicas adaptadas às necessidades locais, visando romper com a dependência estrutural das grandes plataformas e possibilitar uma emancipação digital para as nações periféricas (CASSINO; SILVEIRA; SOUZA, 2021 p. 59).

Na sequência, Débora Franco Machado, em *Dados como produto das operações das mídias sociais no Sul Global*, explora a colonização de dados como um processo que vai além do uso passivo das redes sociais, entendendo-o como um instrumento de dominação estrutural das *big techs* sobre populações do Sul Global. Ela destaca que a expressão "colonização de dados" representa a apropriação massiva de dados e sua centralização nas mãos de poucas corporações tecnológicas. Essas corporações, como o Facebook e o Google, implementam uma estrutura de

²²⁵ Amadeu exemplifica essas práticas no contexto brasileiro, analisando o caso do Sistema de Seleção Unificada (SiSU), cuja gestão de dados foi terceirizada para a Microsoft Azure. O Ministério da Educação justificou essa decisão com base na economia de custos, porém, Amadeu alerta para as implicações dessa escolha em termos de segurança e soberania digital. Os dados de milhões de estudantes brasileiros foram enviados para uma corporação estrangeira, destacando como o neoliberalismo e a colonialidade de dados atuam para consolidar a dependência digital do Brasil, que se torna vulnerável ao poder das *big techs*, ao invés de promover a criação de soluções locais e a independência tecnológica (CASSINO; SILVEIRA; SOUZA, 2021, p. 53).

coleta que transforma a vida cotidiana em um recurso comercializável, espelhando práticas do colonialismo histórico ao transformar tudo o que está online em dados coletáveis (MACHADO, 2021, p. 53-54).

Débora Machado também argumenta que o colonialismo de dados não depende da força física como o colonialismo histórico, mas utiliza métodos tecnológicos para manter o controle sobre os usuários. Ela cita que os algoritmos e interfaces das redes sociais modulam comportamentos, influenciando o que os usuários veem e fazem. Por exemplo, o *Facebook* utiliza o “*Social Graph*”, uma ferramenta que mapeia as interações entre usuários e objetos na plataforma, permitindo categorização detalhada dos usuários. Esses dados são armazenados em grandes centros localizados no Norte Global, criando uma estrutura de poder que segrega fisicamente o local de extração do local de controle (MACHADO, 2021, p. 56-57).

Além disso, a autora analisa o papel das empresas de redes sociais na implementação de infraestrutura tecnológica no Sul Global, incluindo iniciativas como o projeto *Free Basics* do *Facebook*, que fornece acesso limitado à internet em regiões menos desenvolvidas. Embora apresentado como uma ação filantrópica, Machado ressalta que esse projeto gera uma dependência digital²²⁶. Ao limitar o acesso a alguns sites e à própria plataforma do *Facebook*, ele restringe a navegação livre, condicionando os usuários a um ambiente digital controlado pela empresa – similar a uma relação de dependência colonial (MACHADO, 2021, p. 62-63).

Por fim, a pesquisadora salienta que, para entender a colonização de dados no Sul Global, é fundamental observar a localização das operações das *big techs*, como a moderação de conteúdo. Essa função essencial para o funcionamento das plataformas é frequentemente terceirizada para países com legislações trabalhistas mais fracas, como Índia e Filipinas. A escolha por essas regiões revela uma continuidade das práticas colonialistas, pois as corporações exploram mão de obra

²²⁶ Débora Machado ainda compara o projeto *Free Basics* à campanha da Nestlé para promover o uso de fórmulas infantis na África e na Ásia nas décadas de 1950 a 1980. Ela argumenta que, assim como a Nestlé induzia uma dependência fisiológica ao desestimular o aleitamento materno, o Facebook cria uma dependência digital ao oferecer acesso controlado à internet. Essa analogia ilustra como o colonialismo de dados se manifesta por meio de estratégias de marketing e infraestrutura digital que moldam o comportamento e as preferências dos usuários em regiões economicamente vulneráveis (MACHADO, 2021, p. 63-64).

barata e expõem trabalhadores a condições prejudiciais, como o trauma psicológico dos moderadores de conteúdo que lidam com imagens violentas sem o amparo legal adequado. Este cenário confirma o papel das redes sociais como agentes de um colonialismo de dados que explora a vulnerabilidade econômica e social das populações do Sul Global (MACHADO, 2021, p. 58-59).

Na mesma obra, o artigo de Rodolfo Avelino, intitulado *Colonialismo Digital: Dimensões da Colonialidade nas Grandes Plataformas*, explora a forma como o colonialismo digital, consolidado pelas grandes plataformas, aprofunda a colonialidade em diversos níveis da estrutura tecnológica. Nesse sentido, Avelino identifica o avanço das tecnologias digitais e das tecnologias da informação e da comunicação como um catalisador para o surgimento de uma nova economia informacional, onde a coleta de dados ocupa um papel central. Esse modelo é possibilitado por algoritmos de alta performance que monitoram e extraem informações a partir de uma gama de interações humanas, como movimentações, preferências e consumo (AVELINO, p. 69). A estrutura dessa economia é orientada pela expansão constante da internet, favorecendo a centralização da renda e do poder nas mãos de corporações multinacionais, com sede majoritariamente nos EUA.

Ao examinar o contexto geopolítico, Avelino traça um paralelo entre o monopólio das grandes empresas de tecnologia – as *big techs* – e as dinâmicas de poder assimétricas associadas ao imperialismo. Inspirado pela análise de Lenin sobre o imperialismo²²⁷, ele sugere que a posição dominante dessas empresas, especialmente as estadunidenses, configura um cenário onde os padrões tecnológicos globais são ditados de maneira unilateral, impondo uma dependência sobre outros países e minando a soberania digital de regiões como a América Latina (AVELINO, p. 71-72).

²²⁷ Nesse sentido, Rodrigo Avelino: “Voltando no tempo, ao analisar as características particulares do capitalismo, Lênin apontava, já no século XIX, como, diante da possibilidade de imensa concentração de capital, o capitalismo se transformaria de tal forma que surgiriam grupos de poderosas empresas que iriam além dos limites de fronteiras nacionais, até se tornarem monopólios gigantescos que submeteriam suas condições a ramos inteiros de produção em escala mundial. Para ele, a etapa anterior à formação desses conglomerados seria a fusão entre o capital bancário e o capital industrial, que daria lugar ao que ele denominou de capital financeiro, que caracteriza a fase imperialista do capitalismo. Suas previsões estavam certas e surge então um novo sistema mundial capitalista monopolista que espalha seus interesses econômicos, políticos e culturais globalmente”. (AVELINO, p. 74).

Avelino cita o sociólogo Michael Kwet para descrever o que chama de "colonialismo empresarial", em que empresas multinacionais estadunidenses colonizam o espaço digital, sem a necessidade de conquista física de territórios. Para Kwet, o colonialismo digital representa a dominação de ecossistemas digitais por empresas dos Estados Unidos em áreas como sistemas operacionais, buscadores, redes sociais, aplicativos de mapas e plataformas de streaming. Essa forma de colonialismo se apropria dos espaços digitais e cria barreiras que dificultam a entrada de alternativas tecnológicas locais, mantendo as economias dependentes e limitando as possibilidades de desenvolvimento tecnológico autônomo (AVELINO, p. 73).

Outro ponto crucial na análise de Avelino – e de especial interesse para o presente escrito – é a ligação entre colonialismo de dados e colonialismo digital. O autor defende que as práticas extrativistas *das big techs*, ao capturar dados pessoais, refletem a lógica colonial de exploração e controle, agora aplicada à esfera digital²²⁸. Inspirando-se em Aníbal Quijano, ele observa que essa prática de coleta e controle de dados reproduz um regime de poder que impõe padrões econômicos, políticos e epistemológicos, semelhante à colonialidade histórica. O domínio exercido pelas *big techs* se expande com a popularização dos computadores, da internet e dos *smartphones*, que inauguram um novo ciclo de colonização digital liderado pelas empresas do Vale do Silício, na Califórnia. Essa região, alavancada por intenso financiamento estatal e políticas de incentivo, tornou-se o centro global das tecnologias digitais e da coleta massiva de dados (AVELINO, p. 74).

Ampliando a análise, Avelino utiliza as ideias de Nick Couldry e Ulisses A. Mejias para afirmar que o colonialismo de dados se diferencia do colonialismo digital, pois se concentra na extração e monetização de dados pessoais em escala global. Essa exploração ocorre em ecossistemas digitais criados para converter dados em capital. Couldry e Mejias descrevem essa prática como o já citado e amplamente explorado "colonialismo de dados", e identificam não um, mas dois polos de poder centralizados: os Estados Unidos e a China. Nessa estrutura, as interações humanas se tornam fontes de lucro, consolidando uma nova forma de exploração onde as

²²⁸ Avelino invoca, nesse aspecto, novamente a teoria de Lênin, no seguinte sentido: "Ao analisar a obra de Lênin, é possível fazer um paralelo ao monopólio das *big techs*, que atualmente influenciam os padrões tecnológicos e de serviços sobre outros povos. Ainda, é possível avaliar esses processos pelas noções do imperialismo, de crescimento rápido das relações de poder assimétricas, sobretudo dos Estados Unidos sobre os países não ocidentais no século XXI". (AVELINO, p. 75).

plataformas digitais transformam a vida social em mercadoria, moldando comportamentos e extraíndo valor econômico de cada interação (AVELINO, p. 75-76).

Além disso, Avelino destaca o papel das plataformas digitais, conforme descrito por Nick Srnicek, que vê essas plataformas como intermediárias das relações digitais e elementos essenciais na extração de dados. Srnicek classifica as plataformas em cinco tipos: de publicidade, nuvem, industriais, de produtos e enxutas, sendo as plataformas de nuvem particularmente importantes, pois oferecem uma infraestrutura que permite o armazenamento e processamento de dados, possibilitando às empresas centralizar a coleta de informações em servidores de alto desempenho. Esse modelo de negócios oferece soluções tecnológicas sob demanda e tem se tornado a opção padrão para o desenvolvimento e armazenamento de sistemas em escala global, consolidando ainda mais o domínio das *big techs* e ampliando o alcance do colonialismo digital (AVELINO, p. 77-78).

Avelino conclui que a infraestrutura digital controlada pelas plataformas corporativas cria um sistema em que os países periféricos ficam economicamente atrelados aos serviços dessas empresas. Diversos pesquisadores, como Van Dijck e Jin, reforçam que as plataformas moldam as relações sociais e organizam a vida dos usuários ao impor um novo modo de viver e interagir, configurando o que Jin chama de "imperialismo de plataforma". Essa forma de imperialismo reforça, mais uma vez, a hegemonia das *big techs* ao ditar os termos de acesso, consumo e organização da vida digital em uma estrutura que remonta às práticas do colonialismo clássico, mas agora por meio da arquitetura digital e da lógica de mercado global (AVELINO, p. 79).

O autor também destaca que as grandes empresas estadunidenses, como Google e Facebook, investem em infraestruturas no Brasil, como cabos submarinos e pontos de presença (PoPs), para reforçar sua presença na infraestrutura física do país e garantir a capacidade de extração e monitoramento de dados locais. Esse controle sobre as camadas físicas da rede é mais um símbolo, entre tantos outros, de uma nova fase de colonialismo, em que as colônias não são mais territórios, mas fluxos de dados transnacionais (AVELINO, p. 83). Para mitigar esse cenário, o autor sugere que é essencial que os países periféricos, como o Brasil, invistam em políticas públicas que incentivem o uso de tecnologias livres, a capacitação em ciência de dados e o

desenvolvimento de infraestruturas autônomas, rompendo, assim, com a dependência estrutural das tecnologias dominadas por grandes corporações (AVELINO, p. 86).

Vê-se, diante de todo esse cenário, que diferentes estudiosos brasileiros têm se dedicado a examinar como o colonialismo de dados afeta especificamente o Brasil, integrando as perspectivas de pensadores como Aníbal Quijano, Nick Couldry e Ulises Mejias. Nos artigos analisados, resta claro como o conceito de colonialismo de dados é analisado como um processo de expropriação digital alinhado ao neoliberalismo, sendo o Brasil um exemplo expressivo dessa realidade. Cassino, *v.g.* utiliza as ideias de Couldry e Mejias para mostrar que o colonialismo de dados constitui uma nova forma de dependência, onde as práticas extrativas digitais replicam a lógica colonial histórica, apropriando-se da vida social e subjetiva para acumulação de capital. Essa prática, comumente executada por grandes corporações de tecnologia dos Estados Unidos, captura informações pessoais e sociais, transformando-as em perfis que, posteriormente, moldam o comportamento dos brasileiros. A quantificação da vida cotidiana e a manipulação desses dados pelo Norte Global reforçam a subordinação tecnológica e cultural do Brasil, enquanto dificultam o acesso a uma soberania digital e autonomia de desenvolvimento (CASSINO, SILVEIRA; SOUZA, 2021, p. 15-18).

Em consonância, Sérgio Amadeu da Silveira aprofunda essa análise, articulando a teoria de Quijano com a lógica neoliberal, argumentando que a permanência da colonialidade se reflete no modo como as tecnologias de dados são geridas, sobretudo no contexto brasileiro. Amadeu explora a ideia de que o neoliberalismo intensifica a dependência das nações periféricas ao transferir as operações e processamento de dados sensíveis para plataformas estadunidenses, como no caso do Sistema de Seleção Unificada (SiSU) do Brasil, cujo processamento é terceirizado para a plataforma *Microsoft Azure*. Tal decisão evidencia uma dependência estrutural que compromete a segurança e privacidade dos dados brasileiros, promovendo uma forma de colonialismo digital em que o país é forçado a delegar o controle de suas informações a empresas externas. Para Amadeu, é essencial que o Brasil adote políticas públicas que incentivem o desenvolvimento de tecnologias próprias e infraestrutura digital autônoma, promovendo uma resistência ao colonialismo de dados e uma recuperação da soberania digital do país (SILVEIRA, p. 37-42; p. 59-60).

Débora Franco Machado, por seu turno, enfatiza a vulnerabilidade do Brasil e de outros países periféricos às práticas extrativas das *big techs*. Machado examina como a "colonização de dados" representa mais do que o uso passivo das redes sociais, sendo, na verdade, um sistema de dominação no qual grandes empresas como Facebook e Google transformam a vida cotidiana em recursos comerciais. A autora destaca que, ao capturar informações sobre os brasileiros sem transparência sobre seu uso, essas plataformas moldam interações e influenciam a percepção dos indivíduos. Em sua análise, a prática dessas corporações reflete as dinâmicas coloniais, ao transferir dados extraídos no Sul Global para o controle do Norte, criando uma nova forma de subordinação. Esse controle é reforçado por iniciativas como o projeto *Free Basics*, do *Facebook*, que oferece acesso limitado à internet, gerando dependência e limitando o acesso a conteúdos que estão fora do ecossistema da própria empresa. Assim, para Machado, o colonialismo de dados se perpetua ao criar uma infraestrutura que restringe a liberdade de navegação e impõe uma espécie de colonialismo digital que relega o Brasil a uma posição de consumo passivo e dependência tecnológica (MACHADO, p. 53-54; p. 62-63).

Rodolfo Avelino, por sua vez, aborda o colonialismo digital de maneira profunda, ligando-o à ideia de imperialismo de plataforma, conceito que destaca como as *big techs* monopolizam os ecossistemas digitais, limitando a autonomia dos países periféricos. Avelino analisa a estrutura das plataformas digitais dominantes, com o Vale do Silício como centro desse poder, argumentando que a posição hegemônica dessas empresas configura um imperialismo moderno, onde o Brasil e outras nações periféricas dependem de plataformas e tecnologias desenvolvidas externamente. Ele aponta que empresas como *Google* e *Facebook* investem em infraestrutura física no Brasil, como cabos submarinos e pontos de presença, consolidando uma rede de extração de dados que se traduz em uma nova forma de colonialismo. Avelino, ao mobilizar as ideias de Quijano e de Couldry e Mejias, destaca que essa relação de dependência perpetua a colonialidade do poder, pois impõe padrões econômicos e tecnológicos do Norte Global, enquanto limita as possibilidades de desenvolvimento autônomo. Para ele, a única forma de romper com essa dinâmica é a implementação de políticas públicas que incentivem o uso de tecnologias livres e o fortalecimento de

uma infraestrutura digital independente, capaz de minimizar a subordinação tecnológica do Brasil e fomentar sua soberania digital (AVELINO, p. 71-73; p. 83-86).

Mas não apenas os autores nacionais – apesar da postura epistêmica elogiável e desejável – pensam a realidade brasileira no que toca ao colonialismo de dados. Os próprios responsáveis por cunhar esse conceito – Nick Couldry e Ulises A. Mejias – mencionam o Brasil em suas obras como um exemplo relevante para entender as implicações globais do colonialismo de dados. Couldry e Mejias citam, por exemplo, logo no prefácio de sua obra *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (2019, Stanford University Press), o caso da integração forçada dos indígenas Bororo, no Mato Grosso, à sociedade colonial por meio da introdução do telégrafo, da cruz cristã e da espingarda. Essa passagem histórica serve como um paralelo para ilustrar como a infraestrutura tecnológica atual impõe novos padrões de dependência e dominação (COULDRY; MEJIAS, 2019, p. 3). No contexto brasileiro contemporâneo, a implementação de tecnologias digitais e a coleta massiva de dados transformam a sociedade de maneira similar, subordinando-a a uma lógica de extração de dados controlada principalmente por corporações estrangeiras, muitas vezes americanas e chinesas.

Assim, Couldry e Mejias utilizam o exemplo do Brasil para demonstrar que a integração forçada a redes de poder colonial, antes realizada por meio de controle físico e territorial, agora ocorre através da tecnologia digital, na forma de colonialismo de dados. Esse processo, como eles apontam, reforça as relações de dependência e de subordinação ao capital global, em um sistema que desvaloriza as populações locais e suas práticas culturais e econômicas (COULDRY; MEJIAS, 2019, p. 36).

Ao longo da obra, novas menções expressas ao Brasil são especialmente notadas. Nesse aspecto, Couldry e Mejias analisam o impacto do colonialismo de dados no Brasil destacando como práticas de empresas de tecnologia configuram uma dependência digital e econômica, similar à dependência observada durante o período colonial. As empresas globais de tecnologia se aproveitam da infraestrutura limitada e das políticas regulatórias ainda em construção para extrair dados e influenciar as esferas sociais e econômicas do país, operando como atores que moldam as preferências e os mercados locais de forma unilateral. Esse modelo cria um ciclo de dependência onde as empresas tecnológicas passam a atuar como

mediadoras essenciais na vida social e econômica, controlando as plataformas e tecnologias às quais os brasileiros têm acesso. (COULDRY; MEJIAS, 2019. p. 213-215).

Essa influência é particularmente evidente em acordos como os de *"zero rating"* que grandes corporações, como o Facebook, firmam com governos e empresas de telecomunicações. Esses acordos permitem o acesso gratuito a determinados serviços de internet, mas ao mesmo tempo centralizam a comunicação e o fluxo de informações em plataformas específicas, promovendo uma "dependência digital" nas infraestruturas controladas por empresas estrangeiras. (COULDRY; MEJIAS, 2019, p. 219-221).

Os autores também destacam a semelhança entre o papel histórico das metrópoles coloniais, que centralizavam informações sobre colônias e distribuía o conhecimento produzido a partir delas, e o papel contemporâneo dos centros de dados internacionais, onde dados coletados no Brasil são processados e monetizados fora de suas fronteiras. Essa estrutura intensifica a dependência, já que o valor agregado gerado pelos dados brasileiros beneficia as sedes dessas empresas, localizadas, em grande parte, fora da América Latina 2019. (COULDRY; MEJIAS, p. 230-233).

A análise detalhada do colonialismo de dados proposta por Couldry e Mejias revela como o capitalismo contemporâneo recorre a estratégias de apropriação da vida humana que se assemelham às práticas coloniais do passado. Ao abordarem o Brasil, os autores demonstram como o colonialismo de dados impacta diretamente as dinâmicas sociais e econômicas no país, exemplificando com práticas de empresas de tecnologia que utilizam dados para influenciar políticas locais e mercados, criando dependência digital e tecnológica semelhante à dependência econômica dos citados tempos coloniais. O conceito amplia o entendimento das dinâmicas de poder e exploração que permeiam a sociedade digital, evidenciando o papel das tecnologias de informação na perpetuação da colonialidade do poder. Para o Brasil, esse conceito tem relevância particular, pois enfatiza como a subordinação histórica se transforma, mas persiste, em novos modos de extração e controle da vida social por meio dos dados.

Diante de todo esse panorama, e com base nos aspectos teóricos analisados, não há como não se concluir que, no contexto brasileiro, a transferência internacional de dados pessoais representa um ponto central na luta pela autonomia e soberania digital. O conceito de colonialismo de dados, ao evidenciar a forma como grandes corporações de tecnologia capturam e processam dados sem a participação efetiva dos países de origem, alerta para a importância de estruturas legais que permitam ao Brasil controlar esses fluxos de informações. A dependência tecnológica que resulta dessa relação impõe ao país a necessidade de regulamentar com rigor as transferências de dados para assegurar que os interesses dos cidadãos brasileiros sejam respeitados. Nesse sentido, o exercício da autonomia legal para definir as condições em que esses dados podem ser transferidos e processados internacionalmente é crucial para evitar que a soberania do país seja comprometida, garantindo que os dados pessoais brasileiros permaneçam sob proteção e supervisão de suas próprias normas jurídicas.

As regulamentações de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD), emergem como ferramentas essenciais para fortalecer essa autonomia. Ao estabelecer diretrizes claras para a transferência de dados pessoais, a LGPD oferece ao Brasil uma base normativa que permite a defesa dos direitos de seus cidadãos em um cenário de crescente exploração digital. Contudo, para que essa autonomia seja efetiva, é fundamental que o país exerça soberania nas decisões de "adequação" ao aceitar ou recusar transferências para países cujas políticas de proteção de dados não sejam consideradas equivalentes. Esse processo de adequação, ao permitir que o Brasil controle com maior rigor o destino de dados sensíveis, assegura que as práticas de tratamento de dados sejam alinhadas aos valores e necessidades locais, evitando que o país se submeta às imposições das corporações e legislações estrangeiras.

O exercício dessa soberania jurídica é particularmente relevante no contexto do Sul Global, onde as vulnerabilidades tecnológicas e econômicas intensificam a dependência de infraestruturas e serviços externos. Ao regular a transferência internacional de dados, o Brasil não só reforça sua autonomia diante do colonialismo de dados, mas também protege sua população contra as práticas extrativistas digitais que visam capitalizar sobre informações pessoais. Isso representa uma resistência

ativa às dinâmicas coloniais contemporâneas, ao passo que promove a emancipação digital, abrindo caminho para que o país desenvolva tecnologias próprias e consolide sua independência frente às grandes plataformas globais.

3.3 Neoliberalismo e imposições econômicas, políticas e culturais ao Sul Global

Consoante se viu, o colonialismo de dados trabalha com a perspectiva de uma hegemonia informacional, na qual o controle e a exploração dos dados se tornam elementos fundamentais para a dominação econômica e cultural. Atua em um mundo globalizado, no qual as transações digitais não conhecem fronteiras, e a disseminação de informações ocorre em uma escala sem precedentes. Nesse contexto, a conectividade global é essencial para um trânsito livre e desembaraçado de dados, permitindo a maximização do lucro por meio da análise, manipulação e comercialização eficazes dessas informações em larga escala. O acesso irrestrito a dados em âmbito global se revela como um fator crucial para o predomínio econômico e a consolidação de poder por parte dos agentes que detêm o controle sobre as plataformas e infraestruturas digitais.

O viés econômico se apresenta como o fio condutor da globalização, compreendida, tomadas as lições de John Gray, como “uma crescente interconexão em vários níveis da vida cotidiana a diversos lugares longínquos do mundo”. (LIMA, *op. cit.*, p. 127). Referido fenômeno teria se iniciado a partir de 1870, uma vez que o incremento do comércio internacional, aliado aos investimentos em infraestrutura logística e de comunicações, permitiu que uma rede primária de relações se estabelecesse entre diferentes regiões do mundo.

Uma ideia mais pujante de globalização ganha corpo a partir da segunda guerra mundial, se consolidando durante a década compreendida entre 1980-1990. As escolas de negócios de grandes universidades estadunidenses passaram a anunciar às grandes corporações, nessa época, um necessário câmbio nas estratégias comerciais, a fim de se adaptarem a uma crescente liberalização e desregulamentação da economia, aliada ao desenvolvimento galopante dos meios de comunicação.

Esse intercâmbio de informações e de relações econômicas, com a dispersão dos elementos produtivos em diferentes locais do planeta, e a realização de importações e exportações de maneira fluida e desembaraçada contribuiu para o declínio do Estado-nação e de seu poder, uma vez que confinado ao território no qual exerce sua soberania, não alcançado diversas relações comerciais que se espraiam para além das fronteiras nacionais.

Diversas empresas, nesse contexto, tomaram o caráter de transnacional, ou, ainda, multinacional, com sinonímia entre os vocábulos. Tais atores comerciais e produtivos se destacam, justamente, por espraiarem suas atividades por diferentes territórios, mantendo uma matriz em determinado país e filiais em tantos outros, a fim de se beneficiar, aqui e acolá, das vantagens econômicas de uma produção barateada, distribuição facilitada e controle administrativo eficaz.

Promove-se, com essa complexidade, uma nova divisão internacional do trabalho²²⁹, em que as etapas produtivas foram dispersadas em vários países, aproveitando as máximas vantagens de cada território, em que o produto final é constituído de várias partes desenvolvidas em diferentes unidades soberanas, que não tem, por conseguinte, o controle sobre a totalidade da produção e da atuação dessas empresas. Há, assim, uma clara limitação política frente ao fortalecimento das

²²⁹ Apesar de o neoliberalismo pregar a flexibilidade do trabalho e a mobilidade como virtudes essenciais, aqueles que tentam exercer essa mobilidade para fugir da miséria ou da perseguição são frequentemente tratados como indesejáveis. Isso ocorre porque, no mundo neoliberal, a mobilidade é privilégio dos capitalistas e dos investidores, enquanto os trabalhadores e os refugiados, que buscam melhores condições de vida ou um simples direito à existência digna, são vistos como ameaças aos recursos e à identidade nacional. Os "migrantes econômicos", que seguem a lógica da "escolha racional" apregoada pelo discurso neoliberal, encontram resistência justamente nos mesmos países que incentivam a flexibilidade laboral de seus cidadãos. Essa hipocrisia reflete a seletividade do sistema, que valoriza a mobilidade apenas quando serve aos interesses econômicos das elites, mas rejeita aqueles que buscam oportunidades por necessidade. Nesse sentido, os refugiados são estigmatizados e associados à ideia de parasitismo ou ameaça à segurança social, quando, na verdade, estão apenas tentando sobreviver dentro das condições impostas pelo próprio sistema que os exclui. O termo "pessoa em busca de asilo", que outrora estava associado ao exercício dos direitos humanos fundamentais, agora carrega um tom pejorativo. Isso demonstra como o neoliberalismo e as políticas de austeridade e fechamento de fronteiras alteraram a percepção pública e política sobre a migração e o refúgio. Governos, especialmente na União Europeia, gastam tempo e recursos buscando formas de barrar a entrada desses indivíduos, em vez de enfrentar as causas estruturais que levam à fuga em massa. A fortificação das fronteiras, uma medida reacionária e seletiva, se contrapõe ao ideal de um mundo globalizado que beneficia apenas os fluxos de capital, mas não os fluxos de pessoas. Essa postura reflete uma crise moral e política: enquanto o sistema neoliberal promove a liberdade econômica e a mobilidade para as elites, ele fecha as portas para os mais vulneráveis, exacerbando as desigualdades globais. Os refugiados, ao serem criminalizados e tratados como números descartáveis, são a prova viva do fracasso do modelo neoliberal em promover qualquer tipo de solidariedade global ou justiça social. Nesse sentido: Bauman, 2007, p. 48.

empresas transnacionais, que não se conectam a nenhum território específico, mas a vários, enfraquecendo a capacidade de os governos atuarem eficazmente para coibir excessos e ilícitos, o que acarreta uma minoração da tutela social por parte do ator legitimamente encarregado de provê-la: o Estado-nação.

A mobilidade do capital se torna, nessa conjuntura, um fator decisivo, tanto na sua capacidade de expandir mercados quanto de evadir responsabilidades. Como bem aponta o sociólogo Zygmunt Bauman, vivemos em uma era onde a mobilidade adquirida pelo capital "desarraigado" não enfrenta mais os limites impostos pelos Estados-nação tradicionais. O capital circula livremente entre fronteiras, sempre em busca de condições mais vantajosas, enquanto suas obrigações com a manutenção das condições de vida e a sustentabilidade das comunidades locais são deixadas para trás.

O resultado dessa mobilidade, portanto, é uma desconexão sem precedentes entre a natureza extraterritorial do poder econômico e a contínua territorialidade da vida cotidiana das populações. Essa desconexão permite que o capital flutue livremente, sem enfrentar os custos das consequências sociais, ambientais ou econômicas de suas atividades. Em vez de se comprometer com as comunidades e enfrentar os desafios de convivência com a "alteridade" — entendida aqui como a resistência ou os interesses locais —, o capital simplesmente se desloca para lugares onde as condições são mais favoráveis, sem resistência ou contestação. Isso reforça a desigualdade estrutural e econômica entre o norte global e o sul global, onde a flexibilidade e mobilidade do capital encontram pouca ou nenhuma limitação administrativa ou regulatória²³⁰.

²³⁰ Zygmunt Bauman, em *Globalização: As consequências humanas*, nos ensina como essa realidade encontra intensa propulsão ao ser impactada pela tecnologia contemporânea: "Também a rede global de comunicação, aclamada como a porta de uma nova e inaudita liberdade e, sobretudo, como o fundamento tecnológico da iminente igualdade, é claramente usada como muita seletividade — trata-se na verdade de uma estreita fenda na parede, não de um portal. (...) Os meios são a mensagem e os meios de comunicação através dos quais está sendo criado o mercado mundial não facilitam, mas ao contrário impedem, o prometido efeito de "gotejamento". Novas fortunas nascem, crescem e florescem na realidade virtual, firmemente isoladas das rudes e despachadas realidades fora de moda dos pobres. A criação de riqueza está a caminho de finalmente emancipar-se das suas perpétuas conexões — restritivas e vexatórias — com a produção de coisas, o processamento de materiais, a criação de empregos e a direção de pessoas. Os antigos ricos precisavam dos pobres para fazê-los e mantê-los ricos. Essa dependência mitigou em todas as épocas o conflito de interesses e incentivou algum esforço, ainda que débil, de assistência. Os novos-ricos não precisam mais dos pobres. Finalmente a bem-aventurança da liberdade total está próxima. A mentira da promessa do livre comércio é bem encoberta; a conexão entre a crescente miséria e desespero dos muitos "imobilizados"

A globalização econômica finca suas bases contemporâneas na teoria denominada de neoliberalismo. Nascida após a segunda guerra mundial e disseminada em países europeus ocidentais e nos Estados Unidos da América, tem como mote um enfrentamento ao Estado Social e sua vontade de prover os cidadãos de direitos sociais e de uma vida de bem-estar. Seus objetivos, definidos a partir dos acordos de Bretton Woods²³¹, foram principalmente três: acabar com a inflação, privatizar, e deixar o mercado regular a sociedade. De acordo com seus fundadores – mais notadamente Friedrich Hayek e Milton Friedman – a regulação do mercado constituía um risco à liberdade política e econômica²³².

Nesse contexto, Hayek acreditava que a concorrência era o mecanismo capaz de coordenar os esforços humanos individuais, e que, uma vez implementada, eliminaria a necessidade de regulação da economia, permitindo, com isso, o desenvolvimento social e econômico por meio da livre produção e livre consumo. Para esse autor, os direitos sociais não eram, *per se*, adversários do neoliberalismo, mas se justificariam, apenas, se seus custos não fossem superiores ao das vantagens obtidas caso se optasse pela livre concorrência. A concorrência funcionaria como o motor do desenvolvimento social, e deveria ser defendida, portanto, com primazia a quaisquer conceitos, a exemplo do dos direitos sociais e mesmo da democracia.

Milton Friedman, por sua vez, advoga que a liberdade política está conectada à liberdade econômica, não podendo florescer sem ela. O sistema de mercado seria capaz de restringir o poder político, não permitindo que ambos se concentrassem nos mesmos entes ou pessoas, e que a implementação de regulações na economia desaguaria, consoante provado historicamente, em conflitos e dissensos.

e as novas liberdades dos poucos com mobilidade é difícil de perceber nos informes sobre as regiões lançadas na ponta sofredora da “globalização”. Parece, ao contrário, que os dois fenômenos pertencem a mundos diferentes, cada um com suas próprias causas marcadamente diversas. Jamais se suspeitaria pelos informes que o rápido enriquecimento e o rápido empobrecimento brotam da mesma raiz, que a “imobilidade” dos miseráveis é um resultado tão legítimo das pressões “globalizantes” quanto as novas liberdades dos bem-sucedidos para os quais o céu é o limite (como jamais se suspeitaria pelas análises sociológicas do Holocausto e de outros genocídios que eles “combinam” perfeitamente com a sociedade moderna, assim como o progresso econômico, tecnológico, científico e do padrão de vida)”. BAUMAN, 1999, p. 78-79.

²³¹ Para uma análise aprofundada dos aspectos políticos e econômicos envolvidos na criação do sistema de Bretton Woods, destacando o papel dos EUA e do Reino Unido nas negociações e a formação do novo sistema econômico global após a Segunda Guerra Mundial, ver IKENBERRY, 1988. Para um enfoque jurídico dos acordos, ver TARULLO, 2004.

²³² LIMA, 2002, p. 158-159.

Para ambos os autores, o Estado, na concepção neoliberal, tem responsabilidades mínimas, com funções reduzidas, como a administração da segurança e da tutela jurídica, sempre visando garantir a liberdade dos indivíduos de atuarem economicamente, mesmo em ambiente internacional, o que contribui para a implementação da globalização. O ideal de livre mercado, portanto, defendido pelo neoliberalismo e adotado por diversos países, contribui decisivamente para o declínio do Estado-nação e de sua política, já que advoga a desregulamentação de um mercado que é transnacional, não permitindo, assim, que cada soberania possa atuar na conquista e defesa dos direitos de seus respectivos nacionais.

Na Grã-Bretanha, o avanço do neoliberalismo sobre os princípios do Estado social foi promovido sob o lema que parecia um slogan de mercado, diretamente associado ao consumo individual. A guinada neoliberal britânica consolidou o que pode ser chamado de uma “ordem do egoísmo”, promovida pelos sucessivos governos conservadores e posteriormente aperfeiçoada pelo “Novo Trabalhismo”²³³. O processo de “modernização”, uma metáfora para a intensificação da lógica de mercado em áreas até então protegidas, tornou-se contínuo. A privatização e a competição se expandiram para setores antes preservados, e o ciclo de modernização tornou-se uma condição permanente das instituições, corroendo a ideia de continuidade e criando um estado de incerteza constante, onde o foco no curto prazo prevalecia sobre planejamentos de longo alcance. O domínio da chamada “mão invisível” do mercado cresceu à medida que o Estado se retirava de áreas cruciais da governança e permitia que as forças de mercado — difíceis de prever, controlar ou regular — ganhassem cada vez mais poder²³⁴.

²³³ Margaret Thatcher, então primeira-ministra, articulou essa visão por meio de frases que ressoavam com os anseios dos cidadãos, como “Quero um médico de minha escolha no momento em que eu desejar”. Esse tipo de retórica moldou a política pública como se os cidadãos fossem consumidores de serviços e não participantes de um projeto social comum. O governo de John Major, sucessor de Thatcher, manteve esse mesmo curso ao introduzir a “carta do cidadão”, um documento que reconfigurava o cidadão como cliente, alinhando-se à filosofia neoliberal de que o mercado deveria moldar todas as esferas da vida. Nesse sentido: Bauman, 2008, p. 180.

²³⁴ Esse, com certeza, foi o maior serviço que a atividade do governo prestou à causa da revolução neoliberal e ao domínio incontestado da “mão invisível” do mercado (“invisível” por se esquivar a todos os esforços para observar, adivinhar ou prever seus movimentos, e muito menos dirigi-los e corrigi-los; a “mão” com que sonha qualquer jogador de pôquer, esperando corretamente que ela seja imbatível). Todas as cicatrizes particulares e os sucessivos turnos de modernização tornaram a mão invisível ainda mais invisível, sempre colocando-a em maior segurança, além do alcance dos instrumentos disponíveis de intervenção política, popular e democrática. Bauman, vida para consumo, p. 151

Esse processo de desregulamentação e privatização enfraqueceu a esfera política. Funções que antes pertenciam ao Estado foram gradualmente terceirizadas ou entregues à iniciativa privada, retirando das mãos da política, e, portanto, do controle democrático, o poder de supervisionar e intervir em setores-chave. A política, antes um campo de ação e resistência popular, passou a ser relegada a uma função passiva, observando a expansão do mercado e suas repercussões sociais.

A narrativa da "modernização" desconsiderou as consequências profundas que esse processo teve sobre os laços sociais e a coesão comunitária. O enfraquecimento das associações e organizações coletivas, que antes serviam como espaços de resistência e solidariedade, resultou na atomização social – não apenas como uma acidental consequência do projeto neoliberal, mas na condição de estratégia deliberada. As reformas neoliberais transformaram os direitos universais em estigmas, e os espaços de trabalho, antes locais de organização coletiva, tornaram-se arenas de competição sem limites claros e definidos²³⁵.

A desconstrução desses mecanismos de autodefesa coletiva deixou a população vulnerável e exposta às dinâmicas de mercado, sem recursos adequados para enfrentá-las. Assim, o neoliberalismo britânico não apenas sobreviveu às sucessivas administrações, mas também consolidou um legado que se expandiu globalmente, impactando as políticas públicas e sociais em todo o mundo, especialmente nos países do Sul Global, onde essas mesmas dinâmicas são replicadas com consequências ainda mais devastadoras.

A crítica de Bauman ao neoliberalismo se fortalece ao examinar, justamente, o papel do Estado no contexto contemporâneo. Ele observa uma aparente contradição: de um lado, a ausência do Estado na regulação de setores cruciais como o financeiro e o bancário; de outro, uma super-regulação nos mecanismos, *v.g.* de seguridade social. Essa dicotomia reflete a profunda transformação do papel do Estado. Enquanto o neoliberalismo promove um "Estado mínimo" que se retira da economia, reduzindo sua intervenção em áreas que impactam diretamente os mercados globais, ele paradoxalmente impõe um Estado "hiper-regulador" nas

²³⁵ Refletidas naquilo que Marilena Chauí chamará de *homogeneização de todas as instituições sociais e políticas*, pautadas, agora, pelos próprios interesses privados e pelo ideal competitivo, na medida em que "todas as instituições sociais e políticas são consideradas organizações de um tipo determinado: a empresa". (CHAUÍ, 2018, p. 420).

esferas que mantêm e reproduzem a hierarquia social e as desigualdades. A figura do Estado, nesse cenário, parece ambígua: ao mesmo tempo presente e ausente, ele reforça a lógica da classe dominante enquanto falha em proteger os mais vulneráveis (BAUMAN, 2010, p. 49-50).

Bauman se refere a essa configuração como uma realidade paradoxal, em que o Estado não atua de maneira equilibrada para todos os cidadãos, mas sim favorece um sistema de classes que perpetua a desigualdade. O Estado, que deveria ter a função de garantir justiça social e prover o bem-estar, transforma-se num agente de manutenção das estruturas sociais existentes, facilitando o fluxo de capital e a acumulação de riqueza nas mãos de poucos. Ao mesmo tempo, exerce um controle rígido sobre os mais desfavorecidos, garantindo que os benefícios sociais sejam mínimos e rigorosamente fiscalizados, sem espaço para generosidade ou compaixão²³⁶.

Nesse cenário, o que emerge é um Estado que não consegue mais exercer sua função original de equilíbrio social, mas que se transforma em um facilitador das forças de mercado, atendendo aos interesses daqueles que têm mais a ganhar com a globalização neoliberal²³⁷. O resultado é a fragmentação da sociedade, onde o tecido social, já desgastado pela precarização do trabalho e pela marginalização de grandes grupos populacionais, cede ainda mais às pressões do capitalismo global, deixando um vácuo de solidariedade e coesão. A "impossibilidade do Estado" que Bauman menciona não é apenas um reflexo de seu fracasso, mas também de seu

²³⁶ Sobre esse aspecto, o sociólogo europeu, em *A ética é possível num mundo de consumidores?* (2013, p. 174): "Nos últimos anos, vivemos uma transformação gerencial no âmbito político, conduzida pelo neoliberalismo. A regulamentação normativa deu lugar à sedução, e o controle panóptico foi substituído pela criação de um estado de incerteza constante, que mantém os indivíduos em precariedade contínua. As políticas de vida, antes reguladas pelo Estado, agora são operadas pelos mercados de consumo, que prosperam na rápida superação de rotinas e na fragilidade dos laços sociais. Esse novo cenário favorece uma cultura de transgressão e experimentação, na qual as normas fixas e estáveis são vistas como obsoletas. Com a ascensão das políticas neoliberais, as antigas visões utópicas de uma vida boa, pública e coletiva foram desfeitas. O espaço público, que servia como palco para engajamentos políticos e sociais, foi gradualmente invadido pela privatização, desregulamentação e individualização. A utopia pública foi substituída por visões individualizadas de felicidade, cada uma adaptada ao consumo pessoal, voltada para prazeres privados, mesmo quando experimentados em conjunto".

²³⁷ Bauman, em sua obra "Em busca da Política", afirma que: "Em vez de cerrar fileiras na guerra contra a incerteza, praticamente todos os agentes institucionalizados eficientes de ação coletiva juntam-se ao coro neoliberal para louvar como "estado natural da humanidade" as "forças livres do mercado" e o livre comércio, fontes primordiais da incerteza existencial, e insistem na mensagem de que deixar livres as finanças e o capital, abandonando todas as tentativas de frear ou regular os seus movimentos, não é uma opção política dentre outras mas um ditame da razão e uma necessidade" (2000, p. 32).

sucesso perverso em manter e reproduzir as desigualdades estruturais. (BAUMAN, 2010, p. 6-7).

A globalização, potencializada pela ideologia neoliberal, ao desconectar o poder do Estado de sua antiga aliança com a nação, impôs uma nova realidade política e social. Tal relação, outrora uma união sólida e central para a governabilidade, tornou-se fragmentada e sujeita a, nos dizeres de Bauman, “flertes extraconjugais” com o capital global. Na nova ordem global, os Estados transferiram grande parte de suas funções e responsabilidades para os mercados internacionais, deixando de lado o papel de protetores exclusivos do interesse nacional. Isso se reflete nas reformas econômicas promovidas por países da Europa Centro-Oriental, que, ao abrir suas economias para o capital global, diluíram as barreiras entre o poder estatal e os fluxos financeiros internacionais, aceitando assim uma forma de dependência econômica²³⁸.

O neoliberalismo, portanto, naturaliza as condições sociais e econômicas, apresentando-as como um desdobramento inevitável das forças de mercado, sem espaço para alternativas ou críticas profundas. A sua ideologia encontra força justamente na rendição ao que é percebido como inevitável: a lógica da produtividade, da competição e dos resultados econômicos. Isso cria uma hegemonia que, paradoxalmente, se sustenta na ausência de crítica e na aceitação passiva do *status quo*.

Ao contrário das ideologias clássicas que buscavam confrontar e, muitas vezes, reverter a lógica das coisas como elas eram, o neoliberalismo subverte essa ideia ao fundir a lógica das coisas com a própria razão. Nesse cenário, a sociedade não mais se questionaria, aceitando a realidade como um dado irrevogável, sem a possibilidade de alternativas viáveis ou práticas críticas que ofereçam novas formas de organização social²³⁹.

²³⁸ Essa dissolução da soberania estatal e da responsabilidade social levou a uma nova configuração política e social, que Zygmunt Bauman descreve como “casais semi-separados”. O Estado e a nação, que antes formavam uma união indissolúvel, agora seguem seus caminhos de forma paralela, mas cada vez mais distantes. Sem o respaldo do Estado como guardião das identidades nacionais e sem as instituições capazes de manter hierarquias sociais fixas, os indivíduos se veem expostos ao livre mercado, onde a construção identitária se torna uma responsabilidade pessoal. Em um ambiente competitivo e fluido, a identidade deixa de ser algo estável e passa a ser uma tarefa constante, um processo contínuo de adaptação, conquistado por meio de esforço individual e recursos próprios.

²³⁹ Bauman recorre, nesse contexto, aos estudos do filósofo francês Jean-François Revel, e aos do filósofo e economista greco-francês Cornelius Castoriadis. Revel, um defensor da racionalidade

O neoliberalismo promove, ainda, um *ethos* centrado no individualismo e na ética do sucesso, criando um ambiente no qual o vencedor é exaltado e a competição é transformada em uma virtude suprema. Essa visão do mundo não apenas limita as alternativas críticas, mas também fragmenta e desregulamenta as forças sociais, deixando-as à mercê de uma lógica de mercado implacável. O caráter autorreferente dessa ideologia faz com que o próprio sistema se perpetue, reforçando a narrativa de que não há outra opção viável.

Nesse sentido, o neoliberalismo se posiciona como um marco conceitual pré-definido, moldando o que pode ou não ser visto, o que é relevante ou irrelevante, e determinando os parâmetros de raciocínio e avaliação. Ele elimina qualquer tensão entre a lógica da razão e a natureza das coisas, tornando-as indistinguíveis. A razão, que nas ideologias clássicas buscava contestar a natureza e as condições sociais, é desautorizada no neoliberalismo, sendo subjugada pela aceitação passiva do que é apresentado como a ordem natural das coisas.

Essa hegemonia ideológica, que naturaliza as desigualdades e os desequilíbrios de poder, tem repercussões profundas nos países do Sul global. O neoliberalismo, ao expandir suas fronteiras e impor suas práticas econômicas e políticas a essas nações, desarticula ainda mais as possibilidades de resistência. A lógica da globalização neoliberal, aliada à economia de vigilância e ao controle dos dados pessoais, transforma esses países em territórios vulneráveis, sujeitos às forças transnacionais que operam sob a bandeira da inevitabilidade econômica. Razão pela qual o neoliberalismo, ao se consolidar como a ideologia dominante, elimina o espaço para o questionamento crítico e perpetua uma lógica de dominação que atinge de forma mais acentuada as regiões periféricas, onde as estruturas de poder locais são enfraquecidas e subordinadas às dinâmicas do mercado global.

científica, acredita que a ciência, por sua natureza investigativa e fundamentada em evidências empíricas, difere profundamente da ideologia. Enquanto a ciência confronta seus postulados com o mundo concreto e os ajusta conforme necessário, a ideologia, como ele sugere implicitamente, faz o oposto: tenta adequar a realidade a suas crenças pré-estabelecidas. Revela a esperança de que a ciência eventualmente substitua a ideologia, o que levaria, conforme a premonição do filósofo Castoriadis, a uma sociedade que já não precisaria se questionar. Castoriadis sugeria que a ausência de questionamento significaria uma estagnação da sociedade, que, ao abandonar o diálogo crítico, estaria sujeita a uma forma de conformismo intelectual, onde a dúvida e o debate seriam substituídos por um consenso passivo. (BAUMAN, 2008, p. 244-245).

Além dos efeitos políticos e econômicos decorrentes das imposições e influências neoliberais, outro aspecto que deve ser destacado é a capacidade de formação de culturas²⁴⁰ e identidades por parte da postura neoliberal.

Uma das expressões mais latentes dessa influência reside na capacidade de o neoliberalismo, por meio da imposição do modo de vida decorrente de sua potente intervenção na realidade, fletir um dos aspectos mais caros à formação dos cidadãos vinculados aos Estados-nação: a própria consciência de orgulho nacional, ou *nacionalismo*. O fervor patriótico, que antes era um recurso valioso e cultivado pelos Estados-nações, agora serve mais ao mercado do que aos interesses estatais. O patriotismo é transformado em mercadoria, vendido em eventos esportivos, shows, e até na *memorabilia* nacionalista. Essa mercantilização do patriotismo atende mais ao lucro de corporações globais do que à construção de um senso de unidade nacional. O Estado, ao terceirizar grande parte de suas funções para o mercado, tornou-se um agente secundário no processo de construção identitária.

Enquanto isso, os indivíduos, à procura de identidade e pertencimento, encontram um Estado cada vez mais incapaz de oferecer as garantias que um dia prometeu. Com a soberania territorial reduzida e o poder político limitado pela lógica do mercado neoliberal, o Estado se afasta de sua função de provedor de direitos

²⁴⁰ Bauman, em *Capitalismo Parasitário* (2010, p. 33-34), reflete que: "feita na medida da liberdade de escolha individual (voluntária ou imposta como obrigação). É destinada a servir às exigências desta liberdade. A garantir que a escolha continue a ser inevitável: uma necessidade de vida e um dever. A assegurar que a responsabilidade, companheira inseparável da livre escolha, permaneça lá onde a condição líquido-moderna a colocou: a cargo do indivíduo, apontado hoje como único administrador da "política da vida". A cultura de hoje é feita de ofertas, não de normas. Como observou Pierre Bourdieu, a cultura vive de sedução, não de regulamentação; de relações públicas, não de controle policial; da criação de novas necessidades/ desejos/exigências, não de coerção. Esta nossa sociedade é uma sociedade de consumidores. E, como o resto do mundo visto bens e reacender constantemente o desejo de substituí-los por outros, "novos e melhorados"; também são necessários para evitar que a insatisfação dos consumidores com um produto em particular se condense num despreço geral em relação ao próprio estilo consumista de vida. Se o mundo habitado por consumidores se transformou num grande magazine onde se vende "tudo aquilo de que você precisa e com que pode sonhar", a cultura parece ter se transformado atualmente em mais um de seus departamentos. Como nos outros, suas prateleiras estão lotadas de mercadorias renovadas diariamente, e as caixas são decoradas com anúncios de novas ofertas destinadas a desaparecer depressa, como as mercadorias que anunciam. Tanto as mercadorias quanto os anúncios publicitários são pensados para suscitar desejos e fisgar vontades (para "impacto máximo e obsolescência instantânea", citando a famosa máxima de George Steiner). Os comerciantes e publicitários responsáveis confiam no casamento entre o poder de sedução das ofertas e o profundo impulso de seus clientes potenciais de "estar sempre um passo à frente dos outros" e de "levar vantagem." Ao contrário da era da construção das nações, a cultura líquido-moderna não tem "pessoas" a cultivar, mas clientes a seduzir".

sociais e políticos plenos. O famoso modelo de direitos proposto por Thomas Marshall – os direitos civis, políticos e sociais – é severamente desmantelado. Os direitos econômicos foram entregues ao mercado global; os direitos políticos são limitados e moldados pela ideologia do mercado livre, e os direitos sociais estão sendo gradativamente substituídos pela responsabilidade individual, em que cada cidadão deve garantir sua própria sobrevivência e sucesso.

A globalização e o neoliberalismo, assim, ao desmancharem as estruturas sólidas que antes definiam a identidade e a soberania, forçou os indivíduos a enfrentarem a fragmentação social e a precariedade de um sistema onde a incerteza e a competição prevalecem. A fluidez das identidades, outrora garantidas pelo Estado, tornou-se uma característica intrínseca da modernidade líquida, em que a busca por estabilidade é incessante, mas raramente alcançada. (BAUMAN, *Identidade*, 2005, p. 35).

O capitalismo global, se já impunha, a partir de tais diretrizes, certos padrões de comportamento aos países periféricos – vide o Consenso de Washington²⁴¹ – passa a ser, na forma assumida mediante as recentes transformações capitaneadas pela importância econômica dos dados pessoais, delineado como “capitalismo de vigilância”, na medida em que pautado em uma “economia de vigilância”, e que, ao deitar seu poder, a partir do centro produtor de tecnologia “leve” e “pesada”, adota as mesmas posturas que outrora: busca controlar, subjugar e “colonizar” a periferia concessiva de dados pessoais.

²⁴¹ "O Consenso de Washington foi a forma como ficou popularmente reconhecido um encontro ocorrido em 1989, na capital dos Estados Unidos. Nesse encontro, realizou-se uma série de recomendações visando ao desenvolvimento e à ampliação do neoliberalismo nos países da América Latina. Essa reunião foi convocada pelo *Institute for International Economics*, sob o nome de "*Latin American Adjustment: How Much has Happened?*", e envolveu instituições e economistas de perfil neoliberal, além de alguns pensadores e administradores de países latino-americanos. Em linhas gerais, não foi preconizada nenhuma medida “inérita” durante o Consenso de Washington, que recebeu esse nome do economista John Williamson em função de sua ampla aceitação pelos países da América Latina, exceto, até então, Brasil e Peru. As ideias desse encontro – tidas como um “receituário”, e não como uma imposição – já eram proclamadas pelos governos dos países desenvolvidos, principalmente EUA e Reino Unido, desde as décadas de 1970 e 1980, quando o Neoliberalismo começou a avançar pelo mundo. Além disso, instituições como o FMI e o Banco Mundial já colocavam a cartilha neoliberal como pré-requisito necessário para a concessão de novos empréstimos e cooperação econômica". Sobre o assunto, ver BATISTA, Mateus Mabelini; CARNUT, Leonardo; MENDES, Aquilas Nogueira. O Consenso de Washington, vulnerabilidade externa e a superexploração do trabalho na América Latina: uma análise à luz da Teoria Marxista da Dependência. De Raiz Diversa: **Revista Especializada em Estudos Latino Americanos**, v. 8, n. 15, 2021, p. 73-109.

A globalização neoliberal tem aprofundado a desigualdade entre o norte e o Sul global, ampliando as disparidades de poder e a exploração dos recursos, inclusive os dados pessoais, nas regiões mais vulneráveis. A liberdade de movimento do capital, garantida pela mobilidade financeira e pela desterritorialização das grandes corporações, é um dos pilares dessa nova ordem econômica. Esse processo, no entanto, não apenas retira a autonomia dos Estados-nação, especialmente os do sul global, mas também intensifica as desigualdades sociais e políticas. A elite global, graças à sua capacidade de mover capital e infraestrutura produtiva livremente, desvincula-se das responsabilidades sociais e econômicas com as comunidades locais, enquanto estas permanecem confinadas às suas territorialidades, sem os mesmos benefícios de mobilidade.

Paul Virilio e outros teóricos contemporâneos destacam como essa mobilidade irrestrita²⁴² é também responsável pela crescente fragmentação das fronteiras e pela criação de novas assimetrias. A velocidade com que o capital se move, aliada ao avanço tecnológico, dissolveu as distâncias geográficas e minou o conceito tradicional de “fronteira”. No entanto, enquanto a elite transnacional desfruta da liberdade de se deslocar e operar globalmente, a maioria das populações, especialmente aquelas localizadas nos países do Sul global, permanece presa às limitações de seus territórios²⁴³, enfrentando dificuldades de acesso a bens e serviços essenciais e sendo excluídas dos benefícios do progresso (BAUMAN, 1999, p. 18).

O neoliberalismo, nesse contexto, exacerba as imposições econômico-políticas sobre os países periféricos, consolidando uma ordem internacional em que a mobilidade e a liberdade de ação são privilégios de poucos, enquanto a maioria permanece confinada a uma realidade de estagnação econômica e marginalização

²⁴² Essa nova mobilidade acentua a desconexão entre o poder econômico e as obrigações sociais. O capital, agora desterritorializado e fluindo livremente entre nações, se exime das consequências sociais e ambientais de sua exploração, deixando para trás comunidades enfraquecidas e desprovidas de recursos. O espaço, como argumenta Bauman, é reconfigurado de modo a atender apenas aos interesses das elites globais, que criam enclaves exclusivos, fisicamente inacessíveis para a população local. Essas novas formas de segregação espacial e social intensificam a fragmentação da vida comunitária e a marginalização das camadas mais vulneráveis da sociedade.

²⁴³ A “liberdade de movimento” das elites globais implica uma ruptura profunda entre o capital e as realidades locais. A mobilidade do capital e da informação reduz a importância das barreiras físicas e culturais, enquanto as comunidades do Sul global permanecem confinadas a suas realidades geográficas, sem os meios para competir ou participar de maneira significativa na economia global. Essa nova ordem neoliberal, portanto, reforça as disparidades existentes, ao mesmo tempo em que desintegra as formas tradicionais de vida comunitária, levando a um processo de exclusão que separa as elites globalizadas das populações locais, agora relegadas a um papel subalterno e marginalizado.

social. As estruturas de poder transnacionais, assim como as corporações globais, moldam um mundo em que o capital se move sem amarras, deixando para trás uma sociedade profundamente desigual, onde a liberdade de movimento, ao invés de ser um direito universal, se torna um privilégio exclusivo da elite global.

No contexto da proteção de dados pessoais, essas transformações são particularmente relevantes. A desregulamentação e a fluidez dos capitais atravessam as fronteiras digitais, impactando a forma como os dados pessoais são tratados e protegidos. A lógica neoliberal, aplicada à esfera digital, pode enfraquecer as tentativas de criar uma governança global de dados que seja justa e equilibrada, desafiando os esforços para manter a segurança e a privacidade dos indivíduos em um mundo cada vez mais interconectado e orientado pelo poder econômico. (Em busca da política, p. 35).

Na contemporaneidade, a crise vivenciada a partir do ano de 2008 figura como o evento mais significativo da crise do neoliberalismo²⁴⁴, e desvela como a “financeirização” e a globalização, ao tempo em que mitigaram a importância das fronteiras para o fluxo do capital, enfraqueceram o poder político dos Estados-nação de, efetivamente, interferirem na economia²⁴⁵.

²⁴⁴ Colapsos financeiros têm lugar em meio a contextos históricos, em conformações discursivas específicas, de caráter econômico, político e moral. As duas maiores recessões ocorridas no espaço de dois séculos têm sido associadas ao processo de longuíssimo prazo de saída da modernidade e a desdobramentos históricos de grande monta - do fascismo e do totalitarismo ao neoliberalismo; do Holocausto à queda do muro de Berlim; do declínio do Estado etnocrático na América Latina à Guerra do Iraque. Ambas as recessões ocorreram no contexto de enormes processos políticos, morais, tecnológicos e militares que não podem ser compreendidos sem a revisão dos arquivos da história e das conformações ideológicas e econômicas que os produziram. (...) Não é o bastante tentar observar, em caráter imediato, as causas e os efeitos econômicos e financeiros do colapso de setembro de 2008; é desejável um exame completo, uma revisão da estrutura que deu forma à nossa abordagem da economia, avaliando, nas encruzilhadas históricas atuais, que instituições sobreviverão e quais podem se tornar redundantes ou mesmo ser "extintas". (Bauman, 2010, p. 6-7.).

²⁴⁵ O neoliberalismo proporcionou uma enorme expansão dos mercados financeiros. As massas de capital financeiro são hoje controladas por administradores de ativos, em grande parte privados, como bancos comerciais e seguradoras, que se fortaleceram, sobremaneira, na era neoliberal. Um dos motores da crise foi o chamado endividamento crescente, tanto das famílias, mas também do setor financeiro, característica própria do período neoliberal. O setor financeiro surge, nesse contexto, como grande tomador de empréstimos durante o neoliberalismo, superando, no ano de 2008, $\frac{3}{4}$ dos tomados pelas famílias e pelo governo em conjunto, e mais do que cada um deles, separadamente. O endividamento pode ser também explicado a partir das fontes de financiamento muito exploradas na era neoliberal, a exemplo dos *comercial papers* lastreados em ativos, que representa a principal fonte de financiamento de *conduits*. Isso representa, trocando em miúdos, a exploração do mercado financeiro, com a obtenção de lucros mediante a diferença da rentabilidade dos títulos de curto prazo emitidos e os de longo prazo adquiridos. Outro multiplicador de lucratividade dos tempos neoliberais é a chamada *alavancagem*, em que certas empresas são compradas, reorganizadas, muitas vezes divididas, e, depois, vendidas por valor superior ao que adquiridas, em mais um exemplo contundente

A larga expansão dos mecanismos financeiros globais, atrelados à perspectiva neoliberal, diminuíram os poderes estatais de efetivamente definir suas políticas macroeconômicas. Construiu-se, portanto, uma estrutura frágil, que funcionou bem para as classes mais altas, para as instituições financeiras e para os gestores do capital, mas que em razão da crise de 2008, mostrou-se pouco funcional²⁴⁶. O aumento da renda de uma minoria – as classes mais altas, se deu em troca da desregulamentação financeira; com a crise, desvelou-se a fragilidade do sistema e a insuficiência do modelo neoliberal de retroalimentar-se sem que desembocasse em crises econômicas.

Os riscos inerentes à livre movimentação internacional do capital já haviam sido anunciados por Keynes, em 1944, e eram conhecidos quando dos acordos de Bretton Woods. Alguns mecanismos de controle foram anunciados naquela época, nunca completamente aceitos pelos Estados Unidos da América, e paulatinamente enfraquecidos, até a liberalização acontecida nas décadas de 1970 e 1980. Em resumo, os mecanismos que governam a economia global contemporânea estão em desacordo com as recomendações de Keynes e com os objetivos originais de Bretton Woods.

A crise econômica e política que domina o cenário contemporâneo estabelece, de acordo com Bauman, uma hegemonia cultural que denomina de "hegemonia da necessidade". Essa hegemonia não apenas transcende as contradições e falhas internas do neoliberalismo, mas também ultrapassa qualquer análise racional de causa e efeito. É como se, mesmo diante de evidências concretas da contribuição do próprio neoliberalismo para a crise, a fé cega nessa ideologia permanecesse inabalada, quase como uma superstição coletiva. Essa fé resiste à realidade não por ser uma visão imbatível, mas talvez porque as alternativas sejam

da financeirização. Um último elemento de financeirização merece referência: os chamados derivativos, representados por contratos financeiros em que um pagamento deverá ser feito a outrem na ocorrência de um evento futuro pré-determinado. Exemplos desses derivativos são o preço de uma ação na bolsa de valores, de uma *commodity*, ou mesmo a taxa de câmbio de alguma moeda. Sobre o assunto, ver Harvey, 2008.

²⁴⁶ Consoante sobredito, a desregulação exerceu papel fundamental em todo esse panorama neoliberal de crescente importância do capital financeiro. Facilitou-se as transações financeiras e as concessões de empréstimo internacional. Nenhuma legislação internacional veio substituir as antigas leis nacionais sobre o sistema econômico. A busca incessante pelo aumento dos níveis de renda e fluxos baseados em excedentes fictícios, entre outros, aliados à desregulação, proporcionaram uma desestabilidade macroeconômica, em que as políticas monetárias dos bancos centrais dos Estados-nação e as políticas fiscais mostram-se insuficientes para lidar com os problemas neoliberais supranacionais.

muito fracas ou, simplesmente, por estarem tão fragmentadas que não conseguem se firmar como respostas consistentes.

Essa “hegemonia da necessidade” é expressa não por ideias ou teorias, mas por números e porcentagens. Parâmetros financeiros são elevados ao status de símbolos incontestáveis, sem a necessidade de justificação, e substituem a política tradicional. Esses números não são apenas ferramentas para descrever a realidade econômica; eles se tornam a própria política – uma política desencarnada, destituída de seres humanos, de cultura e, sobretudo, do processo democrático. A política, tal como a entendíamos, deixa de ser um campo de competição entre sujeitos e ideias, onde o julgamento eleitoral e o debate público moldavam o poder. Ao invés disso, a política se reduz a um processo técnico e automatizado, que obedece apenas às diretrizes financeiras, sem qualquer preocupação com o consenso ou com a participação democrática.

O grande problema dessa hegemonia dos números é que, ao tomá-los como indicadores supremos, ignoram-se os processos e os caminhos que levam aos resultados. Esses parâmetros financeiros não se preocupam com as implicações sociais, culturais ou políticas das medidas adotadas para alcançá-los. Não há espaço para o diálogo democrático, para o debate sobre como esses objetivos são alcançados, e muito menos para a verificação contínua do poder à luz da participação popular, que é a essência da política democrática.

No coração dessa questão está o problema do consenso, que é fundamental para a sobrevivência de qualquer regime democrático. A informação, o conhecimento e a participação são os pilares que sustentam uma democracia viva e funcional, e, no entanto, a política neoliberal os ignora em prol de uma suposta eficiência técnica. O resultado é uma despolitização crescente da sociedade, em que a democracia é esvaziada de seu conteúdo participativo, e o poder é confinado a um círculo fechado de especialistas e tecnocratas, isolados do debate público.

A partir disso, surge a pergunta: o que fazer diante desse cenário? A política foi sequestrada pelos números, e o neoliberalismo, que outrora era apenas uma ideologia econômica, tornou-se uma espécie de "Constituição material", moldando todas as esferas da vida pública. A política contemporânea perdeu sua alma, sua capacidade de articular interesses legítimos em torno de valores e ideais que vão além

do mero cálculo econômico. A história, a tradição, as paixões coletivas e os valores que, no passado, faziam as bandeiras das nações tremularem, parecem ter sido suprimidos por essa lógica fria e desumana dos parâmetros econômicos. (BAUMAN, 2016, p. 64-65).

Os impactos do neoliberalismo no Brasil foram profundos e multifacetados²⁴⁷, afetando diversas esferas da sociedade, especialmente a economia, o papel do Estado e as relações de trabalho. No final do século XX, com a implementação das reformas neoliberais durante o governo de Fernando Collor de Mello e, posteriormente, intensificadas no governo de Fernando Henrique Cardoso, o país vivenciou um processo acelerado de privatizações, desregulamentações e redução do papel do Estado na economia. A retórica neoliberal, baseada na ideia de que o mercado deveria ser o principal regulador das atividades econômicas, influenciou a política brasileira de maneira decisiva, promovendo a abertura da economia ao capital estrangeiro e a liberalização das finanças.

Um dos principais impactos dessas reformas foi a desindustrialização progressiva e a diminuição do investimento em setores estratégicos da economia, como a infraestrutura e a tecnologia. Ao contrário do que propunha a doutrina neoliberal, que defendia que a privatização e a competição trariam eficiência e crescimento, o Brasil testemunhou o aumento das desigualdades sociais e a precarização das condições de trabalho. O mercado de trabalho tornou-se mais flexível, o que na prática significou maior informalidade, contratos temporários e a diminuição dos direitos trabalhistas.

Além disso, o neoliberalismo no Brasil intensificou a dependência do país em relação ao capital internacional. A desregulamentação dos fluxos financeiros e a liberalização da economia facilitaram a entrada de investimentos estrangeiros, mas, ao mesmo tempo, tornaram o país vulnerável às flutuações do mercado global. Essa vulnerabilidade ficou evidente nas crises econômicas que abalaram o país, como a crise cambial de 1999 e a crise financeira de 2008, ambas exacerbadas pela falta de mecanismos de proteção estatal. A redução da capacidade do Estado de intervir na

²⁴⁷ Sobre os impactos do neoliberalismo no Brasil, recomenda-se os escritos de Sader, (2013); Souza, (2017); Paula; Pereira, (2020).

economia agravou a instabilidade financeira e comprometeu a capacidade do governo de implementar políticas sociais robustas.

No campo social, as políticas neoliberais no Brasil contribuíram para a retração das políticas públicas voltadas ao bem-estar social. A Reforma da Previdência e a Reforma Trabalhista, por exemplo, ambas implementadas no século XXI, são exemplos de como o neoliberalismo buscou reduzir o papel do Estado na provisão de direitos sociais. Essas reformas reduziram a proteção social e ampliaram a responsabilidade individual dos cidadãos, seguindo a lógica neoliberal de que a intervenção estatal deveria ser mínima. Ao passo que o mercado assumiu um papel central, a desigualdade social e a pobreza se intensificaram, demonstrando as falhas dessa abordagem em lidar com as questões estruturais da sociedade brasileira.

Por fim, o avanço do neoliberalismo no Brasil, assim como em outras partes do mundo, não se restringe à esfera econômica. Ele também afeta a política e a democracia. A crescente influência do mercado sobre as decisões governamentais resultou em um distanciamento entre o poder político e a sociedade civil, uma vez que as políticas públicas passaram a atender prioritariamente os interesses do capital financeiro e das grandes corporações. Esse processo de alienação da população em relação às decisões econômicas e políticas fortaleceu o sentimento de descrença nas instituições democráticas, criando um terreno fértil para o surgimento de movimentos populistas e autoritários.

Essa mesma lógica de desregulamentação atravessa o campo da proteção de dados pessoais, com implicações significativas no Sul global. As nações periféricas, como o Brasil, têm menos capacidade de influenciar as regras globais que regem a economia digital. O colonialismo de dados – conceito que aponta para a exploração desigual de dados pessoais por grandes corporações internacionais – intensificou essa relação de dependência. As empresas de tecnologia do Norte global controlam vastas quantidades de dados coletados em países do Sul global, utilizando-os para maximizar lucros, enquanto os governos dessas nações têm pouca capacidade de regular esse fluxo.

No Sul global, o neoliberalismo exacerbou as desigualdades estruturais, permitindo que as corporações transnacionais, muitas delas com sede no Norte global, se beneficiem das fragilidades regulatórias locais para explorar recursos e

dados. A liberalização do mercado de dados – facilitada pela internet e pelas plataformas digitais – possibilita que informações pessoais circulem globalmente sem restrições claras, colocando em risco a privacidade dos indivíduos e reforçando a concentração de poder nas mãos de poucas empresas.

Além disso, o neoliberalismo e sua ideologia de mercado livre promovem a ideia de que a regulação estatal é um entrave à inovação. Esse discurso frequentemente encontra apoio em setores da economia digital que resistem a regulamentações mais rígidas sobre a proteção de dados. No entanto, essa visão ignora as implicações éticas e sociais da exploração desenfreada de dados, especialmente em países onde a cidadania digital ainda não está plenamente desenvolvida e onde a maioria da população não tem acesso a mecanismos robustos de defesa contra violações de privacidade.

No Sul global, portanto, o neoliberalismo se manifesta não apenas como uma força econômica, mas também como uma estrutura de poder que molda a relação entre os cidadãos e o mercado digital. A ausência de um arcabouço regulatório forte e independente que proteja os dados pessoais coloca as populações dessas regiões em uma posição vulnerável frente ao poder das corporações globais.

Em âmbito nacional, inclusive, se sobrepõem os estudos sobre os impactos do neoliberalismo a partir das reflexões de Marilena Chauí. A partir das reflexões da filósofa brasileira, é possível aprofundar a análise dos impactos do neoliberalismo no Brasil e no Sul global, evidenciando como essa doutrina não apenas redefine as dinâmicas econômicas, mas também subverte os princípios democráticos e sociais.

Chauí descreve o neoliberalismo como uma força que reduz drasticamente o espaço público e democrático, substituindo-o pela lógica de mercado e pela expansão do espaço privado. No Brasil, essa transição foi particularmente notável com o enfraquecimento das políticas públicas e a transformação dos direitos sociais em mercadorias, acessíveis apenas no mercado. A retirada do Estado das áreas de saúde, educação e outros direitos sociais básicos reforçou a segregação social, tornando o acesso a esses direitos um privilégio, em vez de um direito universal²⁴⁸.

²⁴⁸ Nesse sentido, Marilena Chauí: “Todavia, no capitalismo, são imensos os obstáculos à democracia, pois o conflito dos interesses é, na verdade, expressão do fundamento mesmo da divisão social, ou seja, a contradição entre o capital e o trabalho e, portanto, a exploração de uma classe social por outra. Assim, por exemplo, se é verdade que as lutas populares nos países do capitalismo central ou metropolitano ampliaram os direitos dos cidadãos e que a exploração dos trabalhadores diminuiu muito,

Além disso, Chauí ressalta que o neoliberalismo reforça a ideologia da competência técnico-científica, gerando uma divisão social que coloca no poder aqueles considerados “competentes” – usualmente alinhados aos interesses econômicos – e marginaliza os “incompetentes”, que são excluídos das decisões políticas e sociais. Esse aspecto do neoliberalismo fortalece a exclusão das classes populares das esferas de decisão, contribuindo para um distanciamento crescente entre o governo e a sociedade civil, no qual os interesses financeiros sobrepõem as necessidades da população. No contexto brasileiro, essa divisão tem ampliado as desigualdades e criado obstáculos para a verdadeira participação democrática, uma vez que o conhecimento técnico-científico se torna um mecanismo de dominação, restringindo o poder político a uma elite dominante.

Chauí também aponta para a influência dos meios de comunicação de massa, que, alinhados aos interesses do capital privado, controlam e produzem informações de maneira a reforçar a ideologia neoliberal e desmobilizar as resistências populares. Esses meios constroem uma narrativa que apresenta o neoliberalismo como uma solução racional e inevitável, minando a crítica e dificultando a participação política autêntica. Essa dominação informacional é particularmente prejudicial nas nações periféricas, onde a comunicação de massa molda a percepção pública e minimiza o papel da sociedade civil na política, ao mesmo tempo que contribui para a alienação da população quanto às decisões que afetam suas vidas diretamente (CHAUÍ, 2018, p. 420).

No cenário da proteção de dados, a visão de Chauí ajuda a compreender como o neoliberalismo, ao promover a privatização e a desregulação, fortalece o colonialismo de dados. A ausência de regulação permite que corporações internacionais explorem informações pessoais coletadas nas nações do Sul global sem restrições, o que submete essas regiões a uma nova forma de exploração

sobretudo com o Estado do Bem-Estar Social, também é verdade, no entanto, que houve um preço a pagar: a exploração mais violenta do trabalho pelo capital recaiu sobre os trabalhadores dos países da periferia do sistema. Por outro lado, também é inegável, em toda parte, a fragilidade dos direitos políticos e sociais sob a ação do neoliberalismo e, portanto, do encolhimento do espaço público e alargamento do espaço privado ou do mercado, sob a forma da privatização e da chamada “desregulação econômica”. Além disso, ao abandonar os investimentos dos fundos públicos nos serviços e direitos sociais e ao destinar os fundos públicos ao aumento da liquidez do capital para o desenvolvimento das novas tecnologias, o Estado neoliberal põe em risco todos os direitos econômicos e sociais conquistados pelas lutas populares”. (CHAUÍ, 2018, p. 419).

econômica. Chauí sugere que o neoliberalismo, ao promover a privatização dos direitos, também transforma o direito à privacidade em uma questão de mercado, no qual apenas aqueles com poder econômico conseguem proteger seus dados. Nesse sentido, o neoliberalismo não apenas facilita a exploração dos recursos digitais dos países periféricos, mas também limita a capacidade desses Estados de garantir a proteção de dados como um direito fundamental.

Ao final, Chauí caracteriza o neoliberalismo como uma forma contemporânea de totalitarismo²⁴⁹, pois homogeneiza todas as esferas sociais e políticas sob a lógica do mercado e da empresa. Todas as instituições, como a escola, o hospital e até o próprio Estado, passam a ser concebidas como empresas, regidas por valores de eficiência, competição e lucro, eliminando o espaço para a pluralidade de interesses e de vozes. Esse totalitarismo neoliberal dissolve o espaço público, restringindo-o ao espaço privado dos interesses de mercado, e desintegra o conceito de sociedade democrática. Tal caracterização oferece uma perspectiva crítica sobre o impacto do neoliberalismo na democracia brasileira, mostrando como ele ameaça os princípios básicos da cidadania e da participação social, e transforma direitos fundamentais em privilégios destinados a uma minoria econômica.

Chauí não é, entretanto, a única a expandir a compreensão de totalitarismo para além dos regimes europeus do século XX. É justamente o sociólogo polonês Zygmunt Bauman, em linha com essa perspectiva, o responsável por também ampliar

²⁴⁹ Marilena Chauí compreende a noção contemporânea de *totalitarismo* de maneira muito acurada, no seguinte sentido: “Para compreendermos essa mutação histórica precisamos compreender que o neoliberalismo é a forma contemporânea do totalitarismo. De fato, núcleo que define a forma totalitária é a homogeneização de todas as instituições sociais e políticas que, sendo idênticas, constituem um todo indivisível. No caso do totalitarismo neoliberal, todas as instituições sociais e políticas são consideradas organizações de um tipo determinado: a empresa. A escola, o hospital, a creche, as artes, o centro cultural, os cultos religiosos são empresas definidas pelas operações de mercado. Nessa perspectiva, Estado também é concebido como empresa e suas ações, definidas pelas regras do espaço privado, isto é, pelo mercado. A essas dificuldades postas pelo capitalismo neoliberal precisamos acrescentar as dificuldades específicas que a sociedade brasileira coloca para a instituição de uma sociedade democrática. De fato, nossa sociedade é marcada pelo predomínio do espaço privado sobre o público e, tendo seu centro na hierarquia familiar, é fortemente verticalizada em todos os seus aspectos: nela, as relações sociais e intersubjetivas são sempre realizadas como relação entre um superior, que manda, e um inferior, que obedece. As diferenças e assimetrias são sempre transformadas em desigualdades que reforçam a relação de mando e obediência. O outro jamais é reconhecido como sujeito nem como sujeito de direitos, jamais é reconhecido como subjetividade nem como alteridade. As relações, entre os que se julgam iguais, são de “parentesco”, isto é, de cumplicidade; e, entre os que são vistos como desiguais, o relacionamento toma a forma do favor, da clientela, da tutela ou da cooptação, e, quando a desigualdade é muito marcada, assume a forma da opressão. (CHAUÍ, 2018, p. 421-422).

o conceito²⁵⁰. Em suas análises, Bauman vê o totalitarismo como uma tendência à “totalidade social”, na qual a busca por uma homogeneização completa do comportamento e do pensamento humano é imposta pelos detentores do poder estatal. Para ele, o totalitarismo não se limita aos governos fascista e nazista, mas manifesta-se sempre que o Estado busca o controle absoluto sobre a conduta dos indivíduos, eliminando a diversidade em favor de uma uniformidade imposta.

Bauman argumenta que a modernidade, com seu foco na burocratização, na racionalização e na ordem social, cria o terreno para a proliferação desses regimes totalitários. Sob essa lógica, as instituições e a sociedade são moldadas para eliminar diferenças, transformando-se em estruturas que promovem uma unidade forçada de pensamento e ação. Assim, os “regimes totalitários” descritos por Bauman refletem não apenas um tipo específico de sistema político, mas também revelam características que ele considera como inerentes ao processo de modernidade, uma verdadeira faceta da racionalidade moderna, que busca ordem e controle total sobre a sociedade como elementos intrínsecos ao processo de modernidade²⁵¹.

Aplicando a lógica de Chauí e Bauman ao neoliberalismo, é possível entender que esse sistema econômico se revela na forma de um totalitarismo contemporâneo, onde a imposição da lógica mercantilista abarca todas as esferas sociais, reduzindo

²⁵⁰ Em parcela considerável de suas obras, visualizamos o dispêndio de especial atenção de Bauman aos estudos conduzidos pela denominada “Escola de Frankfurt”, cujos sociólogos principais eram representados por Theodor Adorno, Max Horkheimer, Herbert Marcuse e Erich Fromm. Além das concepções acerca do espaço e tempo, bem como das mudanças vislumbradas nos sistemas produtivos, Bauman se detém em uma análise pormenorizada dos denominados “anseios modernos”, ou, como prefere indicar, a “tendência totalizante” combatida pela teoria crítica. Esta escola detinha como objeto de estudo a “emancipação”, tendo em vista que a liberdade estava constantemente ameaçada pelo estabelecimento iminente de regimes totalitários, que viriam com o objetivo de aniquilar qualquer possibilidade de autodeterminação e individualidades sociais. Nesse sentido, Zygmunt Bauman leciona que: “Mais uma vez, em retrospecto, podemos dizer que a teoria crítica pretendia desamar e neutralizar, e de preferência eliminar de uma vez, a tendência totalitária de uma sociedade que se supunha sobrecarregada de inclinações totalitárias intrínseca e permanentemente. O principal objetivo da teoria crítica era a defesa da autonomia, da liberdade de escolha e da autoafirmação humanas, do direito de ser e permanecer diferente”. (BAUMAN, 2001, p. 34).

²⁵¹ Bauman reflete sobre tais questões também em “Modernidade e Holocausto”, na medida que afirma: “Toda organização social, quer projetada, quer totalizante (isto é, como campos demarcados de relativa homogeneidade pela supressão ou degradação de todas as outras características diferenciadoras e, portanto, potencialmente divisórias — tornadas irrelevantes ou, de outro modo, sem importância), consiste em submeter a conduta de suas unidades a critérios de avaliação instrumentais ou processuais. Mais importante ainda, consiste em colocar fora da lei todos os demais critérios, primeiro e antes de mais nada padrões que possam tornar o comportamento das unidades resistente às pressões uniformizantes e, portanto, autônomo face ao propósito coletivo da organização (que, do ponto de vista organizacional, os torna imprevisíveis e potencialmente desestabilizantes). (BAUMAN, 1999, p. 238).

o espaço público a uma extensão do mercado. Assim como Bauman critica a modernidade por seu caráter homogeneizador, Chauí identifica no neoliberalismo uma tendência similar de absorção da diversidade social, convertendo instituições sociais, políticas e até mesmo culturais em empresas, estruturadas para atender às demandas do mercado. Nesse cenário, o neoliberalismo se torna uma força totalizante que, ao valorizar a eficiência e a produtividade acima de tudo, elimina as bases de uma sociedade plural e democrática.

Essa leitura, inspirada pelos conceitos de ambos os pensadores, revela que o neoliberalismo busca moldar os cidadãos de acordo com um único ideal de sujeito: competitivo, individualista e motivado pelo lucro. A homogeneização promovida por esse sistema de mercado age como um “regime totalitário”, no sentido cunhado pelo sociólogo polonês, ao reprimir a diversidade de interesses e silenciar vozes que resistem à lógica do mercado. Como aponta Chauí, o Estado e suas instituições perdem autonomia e se submetem ao modelo de empresa, marginalizando a solidariedade e o bem comum. Nessa dinâmica, tanto para Bauman quanto para Chauí, o neoliberalismo constrói uma “totalidade social” que redefine direitos e responsabilidades, transformando cidadãos em consumidores e ameaçando a essência da democracia ao restringir o direito ao dissenso e à pluralidade.

No contexto da proteção de dados pessoais, o Brasil deu um passo importante com a implementação da Lei Geral de Proteção de Dados (LGPD). Referida legislação, ainda que em determinada medida busque equilibrar as referidas relações de poder, estabelecendo regras para o tratamento de dados e tentando proteger a privacidade dos cidadãos, por vezes faz sentir justamente a influência externa interessada em uma postura submissa da realidade nacional. A influência do neoliberalismo se faz sentir na forma como o Estado regula o fluxo de dados em relação às exigências do mercado internacional, refletindo um desequilíbrio de poder entre as grandes corporações transnacionais e a capacidade do governo brasileiro de impor regras que efetivamente protejam os interesses nacionais.

Interpretando de forma ainda mais profunda referidos estudos sobre o neoliberalismo no campo da proteção de dados pessoais no Brasil, percebe-se que a Lei Geral de Proteção de Dados (LGPD), embora tenha como objetivo a defesa da privacidade dos cidadãos, acaba, em muitos casos, reforçando a assimetria de poder

entre as corporações transnacionais e o Estado brasileiro. A própria estrutura normativa da LGPD, especialmente no que tange à transferência internacional de dados, reflete uma concessão à lógica neoliberal: em vez de uma postura de obrigatoriedade e rigidez, a ANPD é dotada de discricionariedade quanto à emissão de decisões de adequação. Essa "flexibilidade", que Chauí e Bauman poderiam criticar como uma subordinação às forças de mercado, permite que interesses econômicos globais influenciem a política de proteção de dados do Brasil, limitando a capacidade do país de garantir uma proteção de dados independente e condizente com as necessidades e interesses nacionais.

A questão da faculdade ou do dever da ANPD em emitir decisões de adequação se torna central nesse contexto, pois envolve um ponto sensível no equilíbrio de poder entre a proteção da privacidade dos cidadãos e as pressões econômicas globais. Ao estabelecer que a ANPD "poderá" reconhecer a adequação de um país ou organismo internacional, o regulamento aprovado pela Resolução CD/ANPD nº 19/2024 abre espaço para uma flexibilidade que, em princípio, pode ser interpretada como necessária diante da complexidade das relações comerciais e diplomáticas internacionais. Contudo, essa mesma flexibilidade pode ser lida como uma vulnerabilidade, permitindo que o Brasil, enquanto nação do Sul global, se veja pressionado a aceitar condições menos rigorosas de proteção de dados impostas por atores econômicos mais poderosos. A ausência de uma obrigação explícita na emissão de decisões de adequação por parte da ANPD cria uma situação em que o interesse econômico transnacional pode se sobrepor ao direito à privacidade dos cidadãos brasileiros.

De forma mais contundente, a decisão da ANPD, ao optar pelo termo "poderá" em vez de "deverá", exemplifica como o neoliberalismo pode infiltrar-se em regulamentos que deveriam, em princípio, assegurar direitos fundamentais, mas que acabam se moldando às pressões externas. Na prática, essa concessão pode abrir caminho para que o Brasil aceite padrões de proteção menos rigorosos em troca de benefícios econômicos ou comerciais, o que Bauman poderia interpretar como uma expressão contemporânea de totalitarismo de mercado. Assim, a crítica de Chauí ao neoliberalismo como um sistema totalizante é especialmente pertinente aqui, pois

aponta para a homogeneização do controle sobre dados, privilegiando interesses de mercado que eclipsam as vozes e as necessidades dos cidadãos.

Essa dinâmica reflete uma questão mais ampla, que é o impacto do neoliberalismo sobre a soberania regulatória dos países do Sul global. A flexibilização das obrigações estatais em áreas estratégicas, como a proteção de dados, aponta para um esvaziamento do poder regulador do Estado em favor da lógica de mercado. O Estado brasileiro, ao adotar essa postura "poderá" em vez de "deverá", transmite um sinal de que sua capacidade de garantir a proteção dos dados pessoais pode ser subordinada às demandas do comércio global. A regulamentação da transferência internacional de dados, repita-se, ao ser permeada por essa linguagem permissiva, revela um risco de que o Brasil acabe se adequando a padrões menos rigorosos de proteção de dados, principalmente para viabilizar acordos comerciais e tecnológicos com países mais desenvolvidos, reproduzindo assim as desigualdades inerentes ao colonialismo de dados.

3.4 Brasil e os desafios frente ao poder, ao neoliberalismo e ao colonialismo de dados: a ANPD e a “decisão de adequação” nacional

No cenário contemporâneo, o Brasil enfrenta uma série de desafios relacionados à proteção de dados pessoais, principalmente no que diz respeito à sua transferência internacional. O neoliberalismo e o colonialismo de dados, em particular, representam forças que buscam subjugar as políticas nacionais aos interesses econômicos globais. Esse fenômeno se reflete na pressão para que países periféricos, como o Brasil, ajustem sua legislação para atrair investimentos de grandes empresas de tecnologia, muitas vezes em detrimento da proteção dos direitos dos cidadãos. Nesse sentido, a Autoridade Nacional de Proteção de Dados (ANPD) ocupa uma posição estratégica, sendo responsável por garantir que a legislação brasileira, especialmente a Lei Geral de Proteção de Dados (LGPD), seja implementada de forma a proteger a autonomia dos cidadãos em um ambiente digital cada vez mais hostil.

O poder no contexto da proteção de dados não se restringe à governança interna do país, mas reflete um campo de tensões em que o Brasil, inserido no Sul

Global, precisa lutar por sua autonomia frente a uma ordem global hegemônica pelo Norte Global. A noção de poder é aqui dupla: implica tanto o poder estatal para regular e proteger dados quanto o poder extraterritorial exercido por corporações e governos estrangeiros que controlam as infraestruturas e os fluxos de dados globais. Assim, a ANPD não atua apenas como uma agência reguladora doméstica; ela se posiciona no epicentro de uma batalha complexa entre proteger a privacidade dos cidadãos brasileiros e mitigar a pressão internacional por práticas de tratamento de dados que favorecem interesses externos.

O neoliberalismo, com sua orientação para a desregulamentação e liberalização de mercados, introduz uma camada adicional de vulnerabilidade no cenário brasileiro. No ambiente digital, o neoliberalismo se manifesta pela promoção de um mercado global de dados, onde a circulação de informações pessoais é tratada como uma commodity, subordinada às regras do livre mercado e controlada, principalmente, pelas grandes corporações de tecnologia. Para o Brasil, essa ideologia neoliberal traduz-se em pressões para que o país flexibilize suas políticas de proteção de dados e aceite a lógica de que o capital – e não o Estado – deve deter o controle das infraestruturas digitais. A ANPD, portanto, precisa resistir a essas forças neoliberais, pois ceder a elas significa abrir mão de uma regulação rigorosa e submeter-se a um mercado de dados que historicamente não favorece os países do Sul Global, mas perpetua uma dependência que outrora era política e econômica, e que agora é também digital.

Em paralelo, o conceito de colonialismo de dados de Couldry e Mejias descreve precisamente essa dinâmica de exploração digital, em que a vida social de populações inteiras é capturada, quantificada e transformada em capital para corporações e governos do Norte Global. Esse novo tipo de colonialismo não exige a ocupação física de territórios; ele opera pela captura e controle dos dados, criando uma subordinação invisível, mas profunda. No caso do Brasil, o colonialismo de dados é evidente nas infraestruturas tecnológicas e políticas que o país utiliza, que muitas vezes são controladas por empresas estrangeiras. Essa dependência resulta em um fluxo de dados sensíveis de brasileiros para centros de processamento e análise de dados no exterior, onde as informações são transformadas em produtos comercializáveis, sem que o Brasil receba os benefícios ou detenha o controle sobre

essas práticas. A ANPD, ao instituir decisões de adequação e estabelecer barreiras à transferência de dados, representa uma tentativa de quebrar esse ciclo e de afirmar a soberania nacional sobre os dados de sua população.

A "decisão de adequação" nacional, portanto, emerge como uma ferramenta crítica para a ANPD e para a soberania do Brasil. Ao regulamentar e limitar a transferência de dados para países que não oferecem proteções comparáveis, a decisão de adequação estabelece uma linha de defesa contra o colonialismo de dados e contra o neoliberalismo digital. Essa medida implica que o Brasil recusa o papel de exportador de dados brutos e exige que os padrões de privacidade e segurança brasileiros sejam respeitados, invertendo a lógica de exploração característica do colonialismo de dados. Para que a decisão de adequação seja eficaz, a ANPD deve adotar critérios rigorosos e transparentes, construídos com base nas particularidades e necessidades do contexto brasileiro, reafirmando o compromisso com uma proteção de dados que preserve a autonomia nacional.

Infelizmente, no entanto, a prática regulatória brasileira ainda não reflete plenamente esse objetivo de autonomia digital, conforme se observa na redação atualmente atribuída ao art. 10 da Resolução CD/ANPD nº 19/2024. Essa redação parece manter uma dependência estrutural, alinhada aos interesses das grandes corporações e dos Estados que historicamente detêm poder sobre o mercado de dados, esvaziando parcialmente o potencial emancipador da LGPD. Em vez de assegurar a proteção rigorosa e a soberania informacional do país, a norma apresenta lacunas que limitam a capacidade de ação da ANPD em um contexto de crescentes práticas extrativistas e pressões neoliberais.

Para que a decisão de adequação cumpra seu papel como um verdadeiro escudo contra o colonialismo de dados, é crucial que a ANPD reveja tais dispositivos e fortaleça os critérios de avaliação. Isso exige não apenas uma revisão técnica, mas também uma postura assertiva de resistência aos interesses externos que buscam manter o Brasil em uma posição subalterna no fluxo global de dados. A autonomia informacional brasileira depende, portanto, de uma ANPD que seja capaz de impor um modelo regulatório robusto, que resguarde os direitos dos cidadãos e que sustente uma infraestrutura digital independente e alinhada às necessidades locais, não subjugada às diretrizes impostas pelo mercado global de dados.

Assim, a atuação da ANPD deve caminhar para um fortalecimento do dever de defesa da soberania digital, exigindo que a decisão de adequação se configure como um instrumento capaz de proteger o Brasil das dinâmicas de poder globais que consolidam o colonialismo de dados. A missão de estabelecer uma política de adequação eficaz não pode ser meramente técnica ou superficial; ela deve refletir uma posição de independência e uma afirmação dos direitos dos cidadãos brasileiros como titulares de seus dados, garantindo que a política de proteção de dados não seja reduzida a uma formalidade regulatória, mas que tenha impacto real na proteção contra práticas extrativas.

Esse movimento em direção a uma independência digital genuína não apenas amplia a segurança e a privacidade dos cidadãos, mas reforça a capacidade do Brasil de atuar como protagonista na ordem digital mundial. Ao construir uma base sólida de proteção de dados, a ANPD possibilita que o país transcenda o papel de fornecedor de dados e atue como um agente ativo e soberano, capaz de influenciar as regras do jogo global e de negociar em pé de igualdade com as grandes potências e corporações globais.

Com isso, o próximo capítulo, "O dever da ANPD e a proteção de dados pessoais: a 'decisão de adequação' brasileira como resposta ao colonialismo de dados", explorará em profundidade a responsabilidade que recai sobre a ANPD para fortalecer sua posição frente aos desafios do cenário digital global, examinando de que forma a decisão de adequação pode se tornar uma ferramenta de resistência e uma resposta eficaz ao colonialismo de dados.

4 O DEVER DA ANPD E A PROTEÇÃO DE DADOS PESSOAIS: A “DECISÃO DE ADEQUAÇÃO BRASILEIRA COMO RESPOSTA AO COLONIALISMO DE DADOS

4.1 O contexto da Lei Geral de Proteção de Dados

No presente capítulo, nos propomos, inicialmente, a uma análise não ortodoxa da legislação protetiva de dados no Brasil; ou seja, não se tecerão, na maior parte desse capítulo, propriamente comentários, críticos ou exegéticos, ao conteúdo dado ao texto da Lei Geral de Proteção de Dados (LGPD), registrada sob o nº 13.709/2019. O exercício interpretativo, próprio de uma textura aberta da linguagem e ínsito ao direito como argumentação²⁵², é enfatizado adiante, mas com finalidade diversa: a de se demonstrar que a atividade criativa do intérprete que busca resolver questões jurídico-normativas atinentes aos problemas nacionais (porquanto vivenciadas por sujeitos nacionais, titulares de bens jurídicos conformados mediante a vivência nacional), ao trabalhar com jogo de linguagem diverso daquele importado a partir do qual se modelou o texto normativo doméstico, dificilmente dará a este sentido idêntico, sob pena de inescapável discrepância com a realidade a ser tutelada.

Analisa-se, desse modo, o processo legislativo que deu azo à edição do texto normativo da Lei Geral de Proteção de Dados (LGPD), destacando-se nele o que há de mais importante e substancial: as justificativas externadas para apresentação dos Projetos de Lei – PL nº 4.060/2012, de iniciativa parlamentar, e PL nº 5.276/2016, de iniciativa do Poder Executivo – para convocação das audiências públicas, para constituição de Comissões específicas e para embasar os relatórios do relator. Após, promove-se uma breve comparação de alguns conteúdos dos textos em si²⁵³, ou seja, da legislação doméstica com aquela que teve como fonte de sua inspiração (ou de submissão): o Regulamento Geral de Proteção de Dados, correspondente à normativa europeia sobre proteção de dados pessoais, registrada como a *Regulation* (EU) 2016/679²⁵⁴.

²⁵² Nesse sentido: Atienza, 2014.

²⁵³ Sem qualquer pretensão de uma comparação integral entre os textos, mas de aspectos capazes de demonstrar similitudes ou diferenças relevantes entre as distintas normativas.

²⁵⁴ Para consulta ao texto integral do RGPD: INTERSOFT CONSULTING. **General Data Protection Regulation - GDPR**. Disponível em: <https://RGPD-info.eu/>. Acesso em: 04 ago. 2023.

A similaridade entre ambas as normas é notável e, muitas vezes, vista como uma forma de alinhar o Brasil às exigências globais de proteção de dados. No entanto, é justamente nesse ponto que surge um dos grandes desafios interpretativos e aplicativos: até que ponto essa inspiração europeia é efetivamente adequada à realidade brasileira? A análise aqui não se limita à mera comparação textual, mas busca problematizar os contextos econômicos, sociais e culturais que moldaram o RGPD e questionar se tais premissas podem ser transpostas para o Brasil sem adaptações profundas. O perigo de reproduzir modelos normativos alheios sem uma crítica contundente reside na possibilidade de se criar uma legislação que, embora formalmente adequada, seja inaplicável ou descolada da realidade social e tecnológica brasileira.

O capítulo se debruça, após, sobre o artigo 34 da LGPD, que trata da "decisão de adequação" para transferências internacionais de dados. Essa disposição, que exige que a transferência de dados pessoais a outros países ou organismos internacionais ocorra apenas quando esses países ou organismos proporcionarem um nível de proteção de dados pessoais adequado, coloca a ANPD no centro do processo decisório. A análise deste artigo é crucial para o desenvolvimento da tese, visto que, mais do que uma simples faculdade regulatória, ele impõe à ANPD o dever de emitir decisões de adequação, como mecanismo de salvaguarda da soberania digital e da proteção dos direitos fundamentais dos brasileiros. Ao fazer isso, o legislador brasileiro reconheceu a importância de se assegurar que as transferências internacionais de dados estejam alinhadas não apenas com os interesses econômicos, mas, sobretudo, com a preservação da privacidade e da dignidade da pessoa humana, pilares centrais do nosso ordenamento jurídico.

Por fim, o presente capítulo apresenta uma análise detalhada do papel fundamental da ANPD na defesa da soberania digital brasileira por meio da emissão das "decisões de adequação", especialmente no contexto da transferência internacional de dados pessoais. Esta análise enfatiza que a ANPD deve não apenas observar o cumprimento formal dos preceitos estabelecidos pela LGPD – algo que a redação hoje atribuída ao art. 10 da Resolução CD/ANPD nº 19/2024 não é, nem ao menos, capaz de fazer – mas, sobretudo, atuar de maneira proativa e estratégica para enfrentar as ameaças do colonialismo de dados e do neoliberalismo digital, que

frequentemente transformam países do Sul Global, como o Brasil, em meros exportadores de dados para centros de processamento globais. Assim, ao adotar uma postura assertiva e criteriosa, a ANPD fortalece o Brasil em seu compromisso com a privacidade e os direitos fundamentais, evitando que as transferências internacionais de dados comprometam a autonomia e os direitos dos cidadãos brasileiros.

Dessa maneira, este capítulo também estabelece uma base teórica e normativa para as análises subsequentes, que detalharão os desafios e as responsabilidades da ANPD na construção de um marco regulatório robusto, capaz de assegurar que as relações de proteção de dados sejam justas e simétricas. Serão exploradas as nuances do dever de emissão de "decisões de adequação" pela ANPD e como essa função se configura como uma barreira essencial contra a exploração extrativa de dados por potências estrangeiras, garantindo que a LGPD não apenas represente um alinhamento formal ao RGPD europeu, mas sim uma resposta genuinamente nacional aos imperativos da proteção de dados pessoais.

Assim, a abordagem crítica adotada neste capítulo visa desconstruir a visão tradicional que enxerga a LGPD como uma mera cópia do RGPD e defender que, no contexto brasileiro, a adaptação crítica do pensamento estrangeiro, ao menos no que toca à transferência internacional de dados pessoais, aliada à autonomia da ANPD em sua função regulatória, é um passo indispensável para garantir que a proteção de dados não seja apenas uma formalidade, mas uma realidade substancialmente aplicada às especificidades do Brasil.

4.2 O processo legislativo da LGPD: inspirada ou submissa?

Em 14 de agosto de 2018, foi publicada, no Brasil, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados. Sua entrada em vigor se deu no mês de setembro de 2020. A LGPD é fruto da junção do Projeto de Lei nº

4.060/2012²⁵⁵, de iniciativa parlamentar²⁵⁶, com o Projeto de Lei nº 5.276/2016, apresentado pela Presidência da República, que gozou de relativa proeminência no texto final aprovado.

Na justificativa apresentada pelo parlamentar para a apresentação do projeto de lei, argumentou que referida normativa visava estabelecer regulamentações para o tratamento de dados pessoais e a proteção dos direitos individuais das pessoas, em resposta ao crescente uso da tecnologia da informação e da internet na sociedade. Buscava-se, assim, tutelar a privacidade e individualidade das pessoas, equilibrando a necessidade de se proteger esses direitos com o da livre iniciativa comercial e de comunicação, reconhecendo a importância de um marco regulatório amplo e abrangente para enfrentar as rápidas evoluções tecnológicas e prevendo um conselho de autorregulamentação para tratar de questões específicas²⁵⁷.

O Projeto de Lei foi objeto de despacho pela Mesa Diretora da Câmara dos Deputados, em 28 de junho de 2012, ocasião em que se determinou o apensamento ao PL-3558/2012, a tramitação em regime ordinário e a sujeição da proposição à apreciação do plenário da casa legislativa²⁵⁸.

Em 2015, o Projeto de Lei relacionado à Lei de Proteção de Dados Pessoais foi submetido à Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados (CCTCI). O Deputado Sergio Zveiter, designado como relator, convocou audiências públicas com representantes de várias entidades e associações²⁵⁹, a fim de discutir os aspectos da lei. A justificativa para essas

²⁵⁵ O PL nº 4.060/2012, de autoria do Deputado Milton Monti (PR/SP), foi apresentado em 13 de junho de 2012, com ementa que dispunha sobre o tratamento de dados pessoais e outras providências. Posteriormente, uma nova ementa foi acrescentada, alterando o foco do projeto para a proteção de dados pessoais e modificando a Lei nº 12.965/2014. **Diário da Câmara dos Deputados**. Disponível em: <https://imagem.camara.gov.br/Imagem/d/pdf/DCD14JUN2012.pdf#page=212>. Acesso em: 04 ago. 2023.

²⁵⁶ Para consulta à íntegra do processo legislativo: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 04 ago. 2023.

²⁵⁷ CÂMARA DOS DEPUTADOS. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750&filename=Tramitacao-PL%204060/2012. Acesso em: 04 ago. 2023.

²⁵⁸ CÂMARA DOS DEPUTADOS. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1006079&filename=Tramitacao-PL%204060/2012. Acesso em: 04 ago. 2023.

²⁵⁹ Entre elas, a Associação Brasileira de Agências de Publicidade (ABAP), Associação Brasileira de Marketing Direto (ABEMD) e da Associação Brasileira das Empresas de Rádio e Televisão (ABERT), além de representantes da Secretaria Nacional do Consumidor - Ministério da Justiça (Senacon/MJ), do Instituto Brasiliense de Direito Público (IDP), e do professor Pablo Ortellado - Professor da Universidade de São Paulo (USP). CÂMARA DOS DEPUTADOS. **Requerimento nº, de 2015. do Sr.**

audiências foi a crescente importância da tecnologia da informação na sociedade e a falta de regulamentação adequada para proteção de dados pessoais no Brasil em comparação com outras nações. Argumentou-se que o país estava atrasado nessa questão, deixando lacunas significativas na proteção da privacidade das pessoas. Os requerimentos foram aprovados em maio e setembro de 2015, refletindo a necessidade de um debate mais aprofundado sobre a proteção de dados pessoais no Brasil.

Designado novo relator, Deputado Sóstenes Cavalcante (RJ), em 12 de novembro de 2015, foi apresentado, em 04 de maio de 2016, o respectivo parecer²⁶⁰.

Em outubro de 2016, uma Comissão Especial foi estabelecida para dar parecer ao Projeto de Lei²⁶¹, com o Deputado Orlando Silva designado como relator. Em novembro e dezembro do mesmo ano, foram apresentados requerimentos adicionais de Audiência Pública pelos Deputados Alessandro Molon (PSB-RJ),

Sérgio **Zveiter.** Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1330147&filename=Tramitacao-PL%204060/2012. Acesso em: 04 ago. 2023.

²⁶⁰ Ante a pertinência, reproduz-se parte de seu conteúdo: “O Projeto de Lei nº 4.060, de 2012, que pretende regular o tratamento dos dados pessoais por parte de entidades públicas e privadas, se alinha às principais legislações sobre privacidade e tratamento eletrônico de dados pessoais em vigência em outros países. De fato, o Brasil demanda uma legislação sobre a matéria, em face do crescimento desse tipo de atividade e da comercialização ilegal desse tipo de informação. Além disso, no ano de 2013 veio a público relato de que as principais empresas de Internet sediadas nos Estados Unidos da América, entre elas o *Google* e o *Facebook*, violam a privacidade de seus usuários, franqueando o acesso a esses dados à NSA, a agência de segurança americana. O Google, especificamente, admitiu que os usuários de seu serviço de e-mail, o Gmail, não têm “expectativa razoável” de que suas mensagens não sejam violadas, e, além disso, afirmou em processo judicial, que corre em corte norte-americana, que “todos os usuários de e-mail devem necessariamente esperar que seus e-mails sejam sujeitos a processamento automático”. Esse contexto, portanto, deixa evidente a premência de uma legislação como a que analisamos. Os termos do projeto estão alinhados com legislações estrangeiras, entre as quais destacamos a Diretiva 95/46/CE da União Europeia, que se aplica aos dados tratados por meios automatizados. (...) O Projeto de Lei nº 4.060, de 2012, portanto, cria um marco legal contemporâneo, estabelecendo os direitos e garantias de privacidade aos usuários, sem inviabilizar a troca e a comercialização dessas informações por parte de entidades públicas e privadas, estabelecendo um regramento mínimo a tais atividades”. CÂMARA DOS DEPUTADOS. Comissão de Ciência e Tecnologia, Comunicação e Informática. **Projeto de Lei nº 4060, de 2012**. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1454623&filename=Tramitacao-PL%204060/2012. Acesso em: 05 ago. 2023.

²⁶¹ CÂMARA DOS DEPUTADOS. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1501981&filename=Tramitacao-PL%204060/2012. Acesso em: 05 ago. 2023.

Orlando Silva (PCdoB-SP), Thiago Peixoto²⁶² (PSD-GO) e André Figueiredo²⁶³ (PDT-CE), com o objetivo de discutir conceitos fundamentais sobre dados pessoais e trazer representantes de várias instituições para contribuir com o debate. Esses requerimentos foram aprovados em novembro e dezembro de 2016, ampliando ainda mais o escopo de discussões em torno do tratamento de dados pessoais no Brasil.

²⁶² Deputado Thiago Peixoto (PSD-GO), apresentou requerimento para que se realizasse Audiência Pública com o representante da Seção Americana do Conselho Empresarial Brasil-Estados Unidos. Como justificativa, indicou que “a Seção Americana do Conselho Empresarial Brasil-Estados Unidos enviou comentários à regulamentação do tratamento de dados pessoais. Nesse sentido, o comparecimento do representante contribuirá para o debate e esclarecimentos sobre o tema em questão”. CÂMARA DOS DEPUTADOS. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1509440&filename=Tramitacao-PL%204060/2012. Acesso em: 05 ago. 2023.

²⁶³ Como justificativas de seu requerimento, assim fez constar o Deputado André Figueiredo (PDT-CE): “O Projeto de Lei em tela possui um importante componente estatal sobre coleta de dados de cidadãos de forma massiva e, às vezes deliberada, especialmente no que se refere à necessidade real dos dados frente aos serviços oferecidos e prestados tanto por pessoas de direito público como de direito privado. Reconhecendo a escala gerada pela Internet, mas que a origem da coleta de dados muitas vezes reside em serviços não eletrônicos – muitas vezes demandados pelo próprio Estado – precisamos dar a oportunidade de manifestação para outros atores não diretamente relacionados ao mundo virtual. Por força regulatória ou por simples coleta deliberada, instituições financeiras e de pagamentos tratam uma grande gama de informações sobre os usuários dos serviços, incluindo dados biométricos, perfis de compra, localização, entre outras. O Banco Central impõe às instituições que exijam de seus clientes uma constante alimentação e comprovação de seus dados e precisa deixar claro para a sociedade a proporcionalidade e a efetividade das exigências sobre o benefício buscado. Da mesma forma, é comum que empresas de análise de crédito, e até do mercado imobiliário mantenham em suas bases de dados informações contidas na declaração de Imposto de Renda dos clientes. Esses extensos cadastros impostos aos usuários muitas vezes não são regidos por qualquer disciplina e alguns, inclusive, são armazenados por empresas terceiras, sem nenhum tipo de compromisso ou controle. Algumas empresas de serviços simples exigem que os clientes forneçam informações cadastrais completas, sob alegação da necessidade para a emissão de Nota Fiscal Eletrônica (uma imposição da Fazenda Nacional) e nada rege a manutenção desses dados em seus sistemas. Pra mencionar um caso mais comum, não é raro vermos prédios públicos ou privados “scanneando” documentos dos entrantes para a liberação do acesso. Com técnicas de OCR e hospedagem de sistemas em nuvem, a vulnerabilidade desses dados é questionável. Assim como também é questionável a efetividade da coleta do dado e o direito de um prédio impor aos transientes o condicionamento do acesso. Que alternativas os cidadãos teriam para a guarda de sua privacidade e qual seria o impacto na segurança? O próprio estado impõe a seus cidadãos (inclusive menores de idade) a coleta de dados biométricos, seja no contexto do processo eleitoral e na participação em exames como o ENEM. Dados biométricos, como a leitura de impressões digitais, estão sendo coletados indiscriminadamente por órgãos públicos, instituições financeiras e até portarias condominiais. Com o avanço da tecnologia e barateamento de coletas mais sofisticadas como dados de DNA, a livre formação de bases de dados desse tipo se torna perigosa e pode representar um problema futuro sem precedentes. Que alternativas são apresentadas aos cidadãos que não querem se submeter a essas coletas? Há um nível elevado de urgência em tratar o tema. O cidadão brasileiro tem o costume de facilmente fornecer seus dados, independente da verificação de boa-fé das empresas ou capacidade de prover a adequada segurança a seus dados. É importante clarificar como a Lei protegerá o cidadão contra abusos e como isso afeta as Relações com os Consumidores. Por fim, há a proposta da existência de um Órgão Competente que precisa ser esclarecida e melhor definida”. (CÂMARA DOS DEPUTADOS. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1509235&filename=Tramitacao-PL%204060/2012. Acesso em: 05 ago. 2023).

Em dezembro de 2016, o Deputado André Figueiredo requereu um Seminário com especialistas internacionais sobre o tema da Proteção de Dados Pessoais²⁶⁴.

Em abril de 2018, a Deputada Bruna Furlan solicitou a realização de uma Audiência Pública para discutir o impacto do uso e da coleta ilegítimos de dados pessoais de brasileiros pela empresa *Cambridge Analytica* através do Facebook, especialmente em contexto eleitoral, e como os Projetos de Lei sob análise poderiam contribuir para prevenir e resolver essas ações inadequadas²⁶⁵.

Em 22 de maio de 2018 – ou seja, três dias antes do início da entrada em vigor do RGPD – é que o Projeto de Lei nº 4.060/2012 recebeu, de seu relator, requerimento de urgência para tramitação²⁶⁶. Referido requerimento foi aprovado em 28 de maio de 2018.

²⁶⁴ Em razão da importância das justificativas apresentadas no requerimento de realização do painel internacional, colaciona-se os argumentos apresentados: “Os trabalhos desta Comissão possuem um importante componente de análise da experiência internacional, não só pelo aproveitamento do conhecimento acumulado dos sistemas de proteção existentes, como pela necessidade de harmonização das normas. Um bom conhecimento da regulação de diversos países é importantíssimo neste momento de elaboração do texto da Lei. A transferência internacional de dados, por exemplo, se dará entre países que possuem marcos legais equivalentes, assim como proposto pelo PL A própria proposta do governo, apensado a esse PL, estabelece que os dados só poderão ser transferidos obedecendo esse princípio. O Brasil não pode ter uma Lei nem mais frouxa nem mais rígida que os demais países, sob o risco de ficar isolado – dados não poderão sair ou entrar – o que poderá limitar muito nossa economia digital”. CÂMARA DOS DEPUTADOS. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1517227&filename=Tramitacao-PL%204060/2012. Acesso em: 05 ago. 2023.

²⁶⁵ A justificativa, ante os argumentos apresentados, é transcrita na íntegra: “Diante do caso recentemente tornado público de utilização indevida, pela empresa *Cambridge Analytica*, de dados pessoais obtidos junto à empresa *Facebook*, e com o intuito de aprofundamento do debate em torno do tema da proteção e tratamento dos dados pessoais, consideramos oportuno convidar, para vir à Comissão Especial de Tratamento e Proteção de Dados Pessoais, os convidados acima mencionados. O sigilo e a privacidade dos dados pessoais de mais de 440.000 brasileiros foram violados no episódio, o que requer desta Comissão o exame mais detido e aprofundado do que realmente ocorreu, de como os envolvidos estão agindo para evitar o mau uso dos dados e como esse tipo de fato pode e deve ser combatido através dos instrumentos legais que estamos ora a analisar e a construir. O importante dever desta Comissão, de votar um Projeto de Lei de Proteção de Dados Pessoais, e também a necessidade de proteção da soberania nacional e da higidez do processo eleitoral, exigem que ouçamos aqueles que estiveram envolvidos mais diretamente no notório episódio de uso indevido de dados. Ademais, é fundamental a apresentação das ações tomadas e em estudo pelas autoridades da Administração. Com esse intuito, a oitiva dos convidados do Facebook, do MPDFT, do TSE e da Senacon mostra-se imprescindível para que essa Comissão Especial possa melhor conhecer os problemas remanescentes e os desafios futuros que recaem sobre a proteção de dados pessoais”. Disponível em: CÂMARA DOS DEPUTADOS.

https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1652716&filename=Tramitacao-PL%204060/2012. Acesso em: 06 ago. 2023.

²⁶⁶CÂMARA DOS DEPUTADOS. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=7940B2663EF5BB140A428FF22B66F40F.proposicoesWebExterno2?codteor=1662254&filename=Tramitacao-PL+4060/2012. Acesso em: 06 ago. 2023.

Logo na sequência, em 24 de maio de 2018, o Relator, Deputado Orlando Silva (PCdoB-SP), apresentou parecer²⁶⁷ pela aprovação do PL nº 4.060/2012, bem como do PL nº 5.276/16, apensado ao anterior. Referido documento conta com 94 (noventa e quatro) páginas, das quais 52 (cinquenta e duas) se dedicam ao relatório e parecer propriamente ditos, e, as demais, ao texto normativo consolidado para aprovação. O relatório e o parecer são integrados, principalmente, por: a) a contextualização de referido Projeto de Lei, b) as audiências públicas e seminários realizados; c) as principais modificações introduzidas pelo Substitutivo; d) a análise das emendas apresentadas ao PL; e e) o texto final consolidado pelo substitutivo.

Ao iniciar seu voto, o Relator salientou a crescente preocupação com a proteção dos dados pessoais ao longo dos anos, tanto na sociedade em geral como na Câmara dos Deputados, ganhando maior destaque após a aprovação do Marco Civil da Internet, instituído pela Lei nº 12.965/2014. Nesse contexto, fez referência a três propostas legislativas que tramitaram em conjunto: a do Deputado Milton Monti, autor da primeira proposta em análise, responsável por abordar a tutela dos dados pessoais, a responsabilidade dos agentes de tratamento e estabelecer conceitos essenciais, como a necessidade de obter consentimento para o tratamento de dados sensíveis e diretrizes claras para a interconexão de dados entre responsáveis; a de autoria do Deputado João Derly, que teve, como foco principal, impedir o compartilhamento de dados pessoais com terceiros sem o consentimento "livre, inequívoco, informado, expresso e específico" do titular, além de apresentar uma definição abrangente, porém concisa, do que constitui dados pessoais; e a terceira, referente à inclusão do PL nº 5.276/16, de autoria do Poder Executivo, que torna a análise, ante o conteúdo analítico do PL, mais complexa e detalhada²⁶⁸.

O Relator fez questão de ressaltar que tais propostas estão inseridas em um contexto global no qual cada país está introduzindo legislações nacionais para tratar da proteção de dados pessoais e garantir a privacidade de maneira harmonizada, uma

²⁶⁷Para consulta ao inteiro teor do parecer: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=Tramitacao-PL%204060/2012. Acesso em: 06 ago. 2023.

²⁶⁸ CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 4.060, de 2012**. Dispõe sobre o tratamento e proteção de dados pessoais. Relator: Deputado Orlando Silva. P. 2-4. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=PRL%201%20PL406012%20=%3E%20PL%204060/2012. Acesso em: 06 ago. 2023.

vez que, de acordo com a mensagem do Poder Executivo, referente ao PL nº 5.276/16, ao todo, 109 (cento e nove) países possuem normas semelhantes, sendo que mais de 90 (noventa) deles têm autoridades públicas especializadas nesse tema. Essa harmonização internacional também criaria, segundo o Relator, um ambiente favorável aos negócios, especialmente para empresas globais que lidam com dados.

Ao realizar o que chamou de “breve contextualização internacional”²⁶⁹, reconheceu que muitas das inspirações para os projetos analisados derivavam do arcabouço europeu. Na Europa, fez menção ao que chamou de primeiro instrumento normativo para proteção de dados pessoais, em referência à Convenção do Conselho da Europa nº 108, de 1981, intitulada "Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automático de Dados Pessoais". Como segundo marco jurídico indicou a Diretiva Europeia nº 46 de 1995, conhecida como Diretiva de Proteção de Dados. Além disso, citou a Diretiva nº 58 de 2002, focada na proteção da privacidade nas comunicações eletrônicas.

Em 2016, a Europa revisou seu sistema com a aprovação do Regulamento nº 679 de 2016, que entrou em vigor em 25 de maio de 2018. Esse regulamento substituiu a Diretiva 95/46 e visa lidar com os avanços tecnológicos e a globalização, estabelecendo um controle mais rigoroso por parte das autoridades de proteção de dados e dando aos indivíduos maior controle sobre seus próprios dados. O regulamento aborda questões como dados sensíveis, genéticos, anonimização, pseudonimização, legítimo interesse e transferência internacional de dados pessoais.

Em contraste, indicou que os Estados Unidos não possuem uma lei específica de proteção de dados, sendo a privacidade tratada como parte da proteção ao consumidor, sob a alçada da FTC (Comissão Federal de Comércio). Aspectos específicos são regulamentados por leis setoriais. Por exemplo, o setor financeiro é regido pelo "Lei de Modernização dos Serviços Financeiros de 1999" e pela "Lei de Análise Justa de Crédito de 1970 - FCRA". Já a proteção de dados de saúde é regulamentada pela "Lei de Portabilidade e Responsabilidade de Seguro de Saúde". A regulação sobre a proteção de dados nos EUA é descentralizada, com diferentes leis para setores específicos²⁷⁰.

²⁶⁹ *Ibidem*, p. 7.

²⁷⁰ *Ibidem*, p. 8.

Em relação à transferência internacional de dados, a Europa não permite que dados pessoais sejam transferidos para países sem legislação que garanta a mesma proteção oferecida pela legislação europeia. Isso levou à criação de acordos, como o "Safe Harbor", que foi revogado em 2015, devido a preocupações com a privacidade dos dados²⁷¹. Em seu lugar, foi implementado o "Privacy Shield", que incluía a supervisão direta do Departamento de Comércio dos EUA sobre empresas que processassem dados de cidadãos europeus²⁷².

Outro acordo relevante seria o CPTPP (Acordo Abrangente e Progressivo para Parceria Trans-Pacífica), formado por 11 (onze) países, incluindo Canadá, México, Japão e Austrália. O Japão, por exemplo, é considerado um país com forte proteção de dados e buscaria se destacar globalmente nesse assunto²⁷³.

Na China, uma força emergente, o tráfego de internet é altamente supervisionado e protegido, com ênfase na *cibersegurança*. A regulamentação de proteção de dados seria descentralizada, semelhante ao sistema dos EUA²⁷⁴.

Essas comparações internacionais foram tidas como importantes para se entender a necessidade de harmonizar a legislação brasileira com padrões globais, ao mesmo tempo em que consideramos nossas especificidades e soberania.

²⁷¹ Em 06 de outubro de 2015, o Tribunal de Justiça da União Europeia, com sede em Luxemburgo e função e de uniformizar a legislação, para que seja interpretada e aplicada da mesma maneira em todos os países integrantes da EU, invalidou, ao julgar o caso Maximilian Schrems v. Data Protection Commissioner, Case C-362/14, o acordo de transferência de dados pessoais até então vigente entre os Estados Unidos e a União Europeia, como "Safe Harbor" ("Porto Seguro", em tradução para o português). (*Ibidem*, p. 10).

²⁷² O Privacy Shield foi um acordo internacional pactuado em 2016, entre Estados Unidos (Departamento de Comércio) e União Europeia (Comissão Europeia), com o objetivo principal de fornecer um mecanismo para que as empresas cumprissem os requisitos mínimos de proteção de dados para transferir dados pessoais do Espaço Econômico Europeu (EEE) para os Estados Unidos. O acordo foi estabelecido para facilitar o comércio transatlântico, garantindo que as empresas respeitassem os padrões de privacidade europeus ao processar ou transferir dados pessoais. No entanto, o Privacy Shield foi revogado pelo Tribunal de Justiça da União Europeia (ECJ) devido a preocupações com a proteção da privacidade das pessoas cujos dados eram transferidos para os EUA. O ECJ considerou que os programas de vigilância dos Estados Unidos não estavam limitados à coleta estritamente necessária e que os titulares de dados não tinham recursos legais nos EUA para contestar a vigilância ou violações de privacidade. Isso levou à conclusão de que o Privacy Shield não fornecia proteção adequada para os dados pessoais transferidos, o que resultou, consoante sobredito, em sua revogação. (*Idem*, p. 10).

²⁷³ *Ibidem*, p. 11.

²⁷⁴ *Idem*.

A partir de tais considerações, passou a analisar as discussões ocorridas durante as audiências públicas e seminários na Comissão Especial que tratou do PL nº 4.060/12 e seus apensos²⁷⁵.

Entre as várias audiências públicas, destacam-se as ocorridas na data de 31 de maio de 2017, que abordou o tópico do órgão competente para a regulamentação²⁷⁶, e na data de 07 de junho de 2017, que tratou da transferência internacional de dados²⁷⁷.

²⁷⁵ A realização de Audiências Públicas e Seminários se revelou, de acordo com o Relator, uma estratégia fundamental diante da intrincada natureza do projeto de lei do Poder Executivo. Os relatores anteriores, inclusive, ao analisarem o PL de forma independente da proposição principal, prontamente reconheceram a necessidade de obter contribuições valiosas dos principais intervenientes no processo.

²⁷⁶ Conforme o Relator, a representante do Internetlab, Beatriz Kira, destacou que havia consenso sobre a necessidade de um órgão regulador autônomo com amplos poderes. Esse órgão seria financiado por taxas do setor, seguindo o modelo adotado no Reino Unido. Além disso, teria dirigentes com mandato fixo e indicações baseadas no critério de notório saber, inspirando-se no exemplo do Canadá. A sabatina também foi mencionada como um importante requisito. Quanto à autorregulamentação, Beatriz Kira ressaltou que ela deveria ser utilizada apenas de forma complementar. Cintia Lima, da USP/RP, mencionou o caso italiano, a Autorità Garanti, composta por parlamentares, como um modelo sujeito a críticas devido à falta de participação da sociedade. Ela também discorreu sobre a importância de regulamentar o mercado relevante relacionado ao "capitalismo informacional" e à monetização dos dados pessoais. Cintia Lima sugeriu que a criação de um órgão independente e autônomo ajudaria a aliviar a pressão sobre o judiciário. Ela propôs um modelo multissetorial semelhante ao Comitê Gestor da Internet no Brasil (CGI), apesar de alegada crise nesse modelo. Alexandre Castro, do Sinditelebrasil, enfatizou a necessidade de uma legislação principiológica e equilibrada, com a liberdade como regra. Ele preconizou uma abordagem de regulação *ex post* e alertou sobre a possibilidade de surgimento de uma "indústria da multa". Alexandre apoiou a criação de um órgão nos moldes de uma agência reguladora e destacou que seu financiamento não deveria sobrecarregar os agentes do setor. Ulysses Machado, do Serpro, observou que a regulamentação também deveria incluir o direito ao esquecimento, a obrigação de garantir a segurança da informação por parte dos agentes de tratamento, além de assegurar o acesso dos órgãos de investigação aos dados cadastrais. Ele enfatizou a importância de alinhar a regulamentação com a Política Nacional de Segurança da Informação e a nova Lei de Identificação Civil. Ulysses sugeriu a criação de uma agência "sui generis" em que os diretores fossem eleitos com mandato. Gabriel Carvalho, do Departamento de Proteção do Consumidor do Ministério da Justiça (MJ), expressou seu apoio à criação de um órgão que representasse a sociedade, com capacidade de fiscalização e investigação. Ele enfatizou que uma agência reguladora, apesar das diferenças em relação à autorregulamentação, seria a solução mais adequada. *Ibidem*, p. 19.

²⁷⁷ Bruno Magrani, do *Facebook*, ressaltou a importância de mecanismos de transferência que permitam a movimentação de dados entre empresas distintas. Ele mencionou o exemplo do Canadá, que permite a transferência de responsabilidade entre empresas. Danilo Doneda, da *Open Knowledge Foundation*, destacou que a proibição do "outsourcing" de dados poderia levar a perdas de investimentos no Brasil. Joana Varon, da Coding Rights, enfatizou a necessidade de um "consentimento forte" e da existência de uma autoridade para remediar e sancionar. Ela alertou para o risco de perda de liberdade e o monopólio na internet, comparando-o ao "colonialismo digital", citando como exemplos a atuação de data brokers, as ações do Google relacionadas a bloqueadores de propagandas e o uso do microfone pelos aplicativos do *Facebook*. Thiago Sombra, da UnB, ressaltou a complexidade em rastrear o tráfego de informações e o papel dos intermediários, o que dificulta a imputação de responsabilidade. Ele apontou a incongruência entre o Brasil ser signatário do CISG (Convenção das Nações Unidas sobre Contratos de Compra e Venda Internacional de Mercadorias) e não possuir uma lei de proteção de dados. Thiago incentivou a autorregulação e correção e sugeriu a sistematização da questão da responsabilidade em uma única seção, verificando sua compatibilidade

Destaca-se, nesse contexto, também a audiência pública realizada em 12 de julho de 2017, responsável por discutir o tema da "Inovação e Indústria 4.0", com clara preocupação relacionada aos investimentos e ganhos econômicos, ainda que demandasse necessárias flexibilizações na legislação protetiva de dados pessoais²⁷⁸.

Além das diversas audiências públicas e conferências sobre o tema²⁷⁹, há que se fazer referência mais específica ao último tópico constante no parecer e no relatório – já que os referentes às “principais modificações introduzidas pelo Substitutivo”, à “análise das Emendas oferecidas ao PL 5.276/16” e as “contribuições recebidas” não serão especificamente tratados, porquanto o primeiro pode ser conhecido mediante os claros reflexos no texto normativo ao final aprovado, o segundo, diante do fato de as emendas, em sua maioria, terem integrado também o texto normativo final (com exceção das de nº 1, 2, 4, 8 e 10²⁸⁰), e o terceiro, pela menção simples e enxuta ao recebimento, no ano de 2018, de um total de 20 contribuições de diversos setores,

com o disposto no Código Civil (Art. 927). Ele também questionou a exclusão da aplicação da lei para transferências internacionais para países não certificados. *Ibidem*, p. 20.

²⁷⁸ O diretor da AMCHAM enfatizou que a legislação de proteção de dados tinha um impacto significativo na segurança jurídica de novos investimentos. Ele criticou os critérios de territorialidade contidos no PL 5.276/2016, argumentando que eles eram excessivamente abrangentes, e defendeu que apenas os dados que realmente identificam o titular deveriam ser considerados como dados pessoais. O presidente da ABES afirmou que a nova lei deveria ter um caráter mais educacional do que sancionatório, pois muitos problemas surgiam devido a falhas e falta de conhecimento dos usuários. Ao destacar a tensão entre a obrigação de transparência e a segurança efetiva dos dados, enfatizou a necessidade de equilíbrio. O Gerente Executivo da CNI ponderou que uma legislação excessivamente detalhada criaria desestímulos ao investimento. Ele também apontou as dificuldades do modelo atual de aplicação das taxas de fiscalização (Fistel) nas comunicações máquina-a-máquina, o que poderia prejudicar o desenvolvimento do mercado de Internet das Coisas (IoT). O representante da ABINEE argumentou que a definição de dados pessoais era muito ampla e poderia gerar confusão. Sugeriu, assim, que apenas dados que realmente identifiquem o titular fossem considerados pessoais. Além disso, questionou a relativização da noção de anonimização, argumentando que a combinação de várias informações poderia levar à identificação do titular, esvaziando o significado de anonimização para fins legais. *Ibidem*, p. 22-23.

²⁷⁹ Entre as conferências, destaca-se a realizada nos dias 10 e 11 de maio de 2017, denominada de “Seminário Internacional de Proteção de Dados Pessoais”. Entre as entidades representantes por diferentes palestrantes, foram destacadas pelo Relator as participações do *US Chamber's Center for Global Regulatory Cooperation – GRC*; da Comissão Europeia; do Governo do Chile e do Departamento de Comércio dos Estados Unidos, entre vários outros. Outra conferência que merece ser mencionada é a representada pelo “Seminário Conjunto de Proteção de Dados Pessoais”, realizado em 22 de maio de 2018, que contou com a participação de diversos especialistas e autoridades na área. *Ibidem*, p. 23-28.

²⁸⁰ As razões pelas quais o Relator rejeitou determinadas propostas de emenda podem ser conhecidas, na íntegra, mediante consulta ao documento. CÂMARA DOS DEPUTADOS. Comissão Especial destinada a proferir parecer ao Projeto De Lei nº 4060, de 2012 (Tratamento e Proteção de Dados Pessoais). **Projeto de Lei nº 4.060, de 2012**. (Apenso PLs nº 5.276/16 e 6.291/16). Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: https://camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=Tramitacao-PL%204060/2012. Acesso em: 06 ago. 2023.

todas devidamente disponibilizadas na página da internet da Comissão Especial. Referido tópico versa sobre o “encaminhamento” dado pelo próprio Relator à questão, o que resultou em um substitutivo às proposições originais, capaz de absorver e condensar as distintas contribuições outrora mencionadas.

Ao fazer suas considerações, o Relator reconhece que estamos imersos em uma nova era, na qual as Tecnologias da Informação e da Comunicação (TIC) não apenas transformaram o cotidiano, mas também inauguraram uma nova dimensão na oferta de produtos e serviços. As TIC permitiram o amplo acesso a serviços essenciais e impulsionaram melhorias na qualidade de vida, sendo o tratamento de dados pessoais o insumo central dessa transformação. A análise de dados possibilita descobrir padrões, prever comportamentos e adaptar resultados, criando oportunidades ainda não totalmente imaginadas.

O Relator alerta, contudo, que grandes corporações e governos acumulam diariamente vastos volumes de dados sobre usuários e cidadãos, o que, sem as salvaguardas adequadas, pode comprometer a privacidade e os direitos humanos, além de ameaçar o princípio democrático. Situações como o uso de dados genéticos para excluir pessoas de serviços ou a coleta de informações locais para perfis de risco são preocupantes. O armazenamento e uso desses dados por empresas, governos e organizações pode impactar diretamente a vida das pessoas, desde o acesso ao emprego e seguros até a manipulação de comportamentos em redes sociais, configurando potenciais danos individuais e coletivos.

Em contrapartida, o Relator enfatiza a necessidade de integrar o Brasil ao cenário global das TIC, aproveitando a proteção de dados como um mecanismo não apenas de segurança, mas também de desenvolvimento econômico e inclusão global. O reconhecimento da proteção de dados no país é, assim, um passo essencial para fomentar o crescimento e tornar o Brasil um ambiente acolhedor para a indústria digital internacional.

Desse embate entre economia de dados vs proteção de dados pessoais, o relator assume uma posição manifestamente favorável à primeira, ao defender que a proteção de dados no Brasil seja encarada como uma oportunidade estratégica para o desenvolvimento econômico e a integração do país ao mercado global de TIC. A legislação de proteção de dados, assim, não deve apenas assegurar a privacidade e

os direitos fundamentais, mas primordialmente fomentar a competitividade nacional, criando condições para que o Brasil se alinhe aos padrões internacionais e se estabeleça como um destino confiável e atrativo para investimentos no setor digital. Esse “equilíbrio” – com expressa predileção à constituição de um ambiente favorável ao investimento estrangeiro em terras nacionais, capaz de se aproveitar dos dados aqui produzidos – entre segurança e inovação é visto como essencial para que o país avance como um parceiro global relevante, capaz de promover um ambiente propício à inovação e à inclusão digital em um mundo cada vez mais interconectado²⁸¹.

Diante desses fatores, o Relator posiciona-se favoravelmente à aprovação das propostas, destacando que o aprofundado exame dos projetos, das contribuições recebidas e das emendas apresentadas revelou a possibilidade de aprimoramentos. Assim, propõe um substitutivo que busca condensar e aperfeiçoar os textos originais, incorporando sugestões que fortalecem a proteção de dados e modernizam a legislação brasileira, e esclarece que pequenas alterações de redação ou técnica legislativa foram realizadas para melhor adequação do texto normativo²⁸².

Por fim, no dia 29 de maio de 2018 – apenas 5 (cinco) dias após a apresentação do Parecer do Relator perante a Comissão Especial, e no mesmo dia em que apresentado referido Parecer perante o Plenário da Casa Legislativa – em votação realizada em turno único, a Câmara dos Deputados apreciou a matéria, aprovando a redação final do Substitutivo assinada pelo Relator, Dep. Orlando Silva (PCdoB-SP)²⁸³. Encaminhou-se, em 30 de maio de 2018, a matéria ao Senado Federal, por meio do Ofício nº 592/2018/SGM-P²⁸⁴.

Em 19 de julho de 2018, a Câmara dos Deputados foi informada, por meio do Ofício nº 925/2018, a aprovação, pelo Senado Federal, com emendas de redação²⁸⁵,

²⁸¹ *Ibidem*, p. 30.

²⁸² *Ibidem*, p. 31.

²⁸³ CÂMARA DOS DEPUTADOS. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1665276&filename=Tramitacao-PL%204060/2012. Acesso em: 07 ago. 2023.

²⁸⁴ CÂMARA DOS DEPUTADOS. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1664774&filename=Tramitacao-PL%204060/2012. Acesso em 07 ago. 2023.

²⁸⁵ Foram apresentadas, no Senado, ao total, 56 (cinquenta e seis) emendas ao texto do PL. Dessas, as de número 2 a 9, de autoria do Senador Valdir Raupp (MDB/RO), foram rejeitadas. A de número 1, apresentada pelo Senador Valdir Raupp (MDB/RO), e as de número 10 a 56, apresentadas pelo Senador Ricardo Ferraço (PSDB/ES), foram aprovadas. A deliberação pelas reprovações e aprovações ocorreram em 03 de julho de 2018, data em que a comissão aprovou o relatório que passou a constituir o parecer da CAE, favorável ao Projeto de Lei da Câmara nº 53 de 2018, com as emendas de redação

do texto normativo, comunicando-se a remessa do PL à Presidência da República, para sanção.

O texto normativo votado pelas casas do Congresso Nacional sofreu, por parte da Presidência da República, veto parcial (MSC 451/18-PE), posteriormente mantido. Assim, em 14 de agosto de 2018, foi, enfim, convertido na Lei Ordinária nº 13.709/2018, veiculada por meio do Diário Oficial da União de 15 de agosto de 2018, p. 59, col. 02. As razões do veto²⁸⁶ foram veiculadas no Diário Oficial da União na mesma data e coleção.

4.3 O texto da Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados (LGPD) do Brasil tem sido objeto de frequentes eventos, seminários e debates, à medida que o país enfrenta os desafios de regular a proteção de dados pessoais em uma era digital²⁸⁷. O detalhamento do processo legislativo que culminou com a promulgação da LGPD cumpre, nesse trabalho, uma função precípua. Mais do que simplesmente relatar a intensa atividade que permeou o procedimento de feitura da LGPD, o que se deve destacar é o que efetivamente se consolidou no texto normativo.

Uma característica distintiva da LGPD é sua semelhança notável com o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia. As semelhanças não passam despercebidas; a LGPD, em vários momentos, parece ser uma adaptação da legislação europeia para o contexto brasileiro. A influência do

supramencionadas, além da rejeição dos Projetos de Lei do Senado nº 330 de 2013; 131 de 2014; e 181 de 2014. Aprovou-se, também, a apresentação de requerimento de urgência para a matéria.

²⁸⁶Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-veto-156214-pl.html>. Acesso em: 07 ago. 2023.

²⁸⁷ A título de exemplo, no ano de 2023, foram realizados eventos pelo Grupo de Estudos de Direito Autoral e Industrial da Faculdade de Direito da Universidade Federal do Paraná. **IV Seminário sobre Proteção de Dados Pessoais. Webinar: 5 anos de LGPD**. Disponível em: <https://www.gedai.com.br/iv-seminario-sobre-protacao-de-dados-pessoais-webinar-5-anos-de-lgpd/>. Acesso em: 08 ago. 2023, pela Ordem dos Advogados do Brasil - OAB Nacional. **Três anos de vigência da LGPD: Os principais avanços na proteção de dados no Brasil - Homenagem a Danilo Doneda**. Disponível em: <https://www.ab.org.br/noticia/61194/oab-abre-seminario-sobre-avancos-da-lgpd-com-homenagem-ao-pesquisador-danilo-doneda>. Acesso em: 08 ago. 2023 e pelo Comitê Gestor da Internet no Brasil. **14º Seminário de Proteção à Privacidade e aos Dados Pessoais**. Disponível em: <https://seminarioprivacidade.cgi.br/>. Acesso em: 08 ago. 2023.

RGPD na LGPD é inegável e revela um desejo de harmonização com os padrões internacionais de proteção de dados²⁸⁸.

No entanto, a influência do RGPD também levanta questões sobre as especificidades e as necessidades do Brasil em relação à proteção de dados pessoais. O país tem suas próprias complexidades e desafios, que talvez não sejam totalmente abordados por um modelo regulatório estrangeiro. A adequação à legislação europeia é evidente em muitos aspectos da LGPD, sem que quaisquer nuances regionais tenham sido consideradas, já que nada aduzem acerca da posição subalterna brasileira no âmbito do poder da privacidade, das imposições neoliberais e do colonialismo de dados – algo especialmente constatado ao relegar à ANPD espaço discricionário por ela compreendido como capaz de afastar seu dever de emitir “decisões de adequação”, afrouxando as garantias nacionais aos cidadãos de que seus dados não serão indevidamente aproveitados por entes estrangeiros, nos casos de transferência internacional de dados pessoais.

Esta semelhança, em grande parte, decorre do desejo de harmonização e da busca por uma adequação eficaz à legislação europeia, visando, principalmente, a facilitar o fluxo de dados pessoais entre o Brasil e a União Europeia, promovendo as relações comerciais. O desejo de assegurar que o Brasil esteja alinhado com os padrões europeus de proteção de dados é uma prioridade que não passou despercebida durante o processo de elaboração da LGPD.

²⁸⁸ Não bastasse as manifestas indicações, durante o trâmite legislativo, da inspiração – que se revela, em razão do viés econômico que dita a aprovação do texto normativo e a posição do Brasil como polo concessivo de dados pessoais e consumidor de tecnologia gestada no estrangeiro, *submissão* – o país conta com várias publicações destinadas à comparação entre os marcos regulatórios, dando conta da influência do RGPD na LGPD. Nesse sentido: IRAMINA, Aline. "RGPD V. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. **Revista de Direito, Estado e Telecomunicações**, v. 12, n. 2, p. 91-117, out. 2020; MENDES, João. A Segurança na Proteção de Dados: entre o RGPD Europeu e a LGPD Brasileira. **Revista do CEJUR/TJSC: Prestação Jurisdicional**, v. 4, n. 8, p. 346-365, 2019; SILVA, Rodrigo Frogeri da; ALEGÁRIO, Cibele Cristina. Os Impactos da Lei Geral de Proteção de Dados (LGPD) no Cenário Digital. **Revista de Direito, Estado e Telecomunicações**, v. 12, n. 2, p. 27-50, out. 2020; BIONI, Bruno Ricardo. Privacidade no Século 21: Proteção de Dados, Democracia e Modelos Regulatórios. **Revista Brasileira de Ciência Política**, n. 41, 2023; ALMEIDA, Daniel F. P. S. de. A proteção de dados pessoais: uma análise da LGPD. **Revista Brasileira de Direito Digital**, v. 10, n. 1, 2020; MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *Comentários ao GDPR*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019; MARTINS, Antônio Eduardo Senna. Comparando a LGPD com a GDPR: abordagens à proteção de dados pessoais. **JusBrasil**, 2023. MARTINS, Antônio Eduardo Senna. Comparando a LGPD com a GDPR: Abordagens à Proteção de Dados Pessoais. **JusBrasil**. Disponível em: <https://www.jusbrasil.com.br/artigos/comparando-a-lgpd-com-a-gdpr-abordagens-a-protecao-de-dados-pessoais/1971798734>. Acesso em: 10 jul. 2024.

A conexão entre a LGPD e o RGPD também tem implicações significativas para empresas multinacionais que operam tanto na Europa quanto no Brasil. Essas empresas podem se beneficiar de uma estrutura regulatória coesa que permite uma abordagem mais consistente à proteção de dados. Ao mesmo tempo, a LGPD deve ser sensível às necessidades específicas do Brasil, de modo a evitar que se torne uma mera réplica do RGPD, sem levar em consideração as peculiaridades latino-americanas, decorrentes de sua posição desfavorável no exercício do poder decorrente da captura e tratamento de dados pessoais, em uma versão renovada do colonialismo.

Nesse sentido, as contribuições de diferentes especialistas, que participaram de várias audiências públicas durante o processo legislativo, são dignas de nota. Muitos especialistas focaram suas abordagens justamente nos ganhos e prejuízos, comerciais e econômicos, advindos de uma adequação da legislação brasileira às expectativas europeias²⁸⁹; alguns experts, por outro lado, manifestaram, de maneira mais intensa, preocupações sobre a abordagem da LGPD em relação aos aspectos da vigilância e do colonialismo de dados na América Latina²⁹⁰.

²⁸⁹ Pode-se citar, como exemplos de manifestações nesse sentido, entre outras, as seguintes: “Danilo Doneda, da *Open Knowledge Foundation*, salientou que o Brasil poderia perder investimentos caso o “outsourcing” de dados não fosse permitido” (p. 20); “O diretor da AMCHAM destacou que a legislação sobre proteção de dados tem impactos significativos na segurança jurídica de novos investimentos. Criticou os critérios da territorialidade contidos no PL 5.276/2016, alegando sua abrangência excessiva, e que os dados que apenas transitam no território nacional, e não pertencem a brasileiros, não deveriam estar incluídos na lei. Na mesma linha, argumentou que códigos de conduta e acordos de cooperação internacional deveriam possibilitar a transferência internacional de dados. Defendeu que somente deveria ser considerado como dado pessoal aquele que realmente identifique o titular.” (p. 22-23); “O Gerente Executivo da CNI ponderou que uma legislação fraca e pouco detalhada gera insegurança jurídica, mas, por outro lado, uma regra demasiadamente minudente criaria desestímulo ao investimento” (p. 23); “A Sra. Natasha Jackson, da GSMA, informou que os dados constituem ativo fundamental muito mais importante que o petróleo porque estes não acabam, são reutilizados e adicionam valor no seu processamento. Para Jackson, regimes restritos impedem a inovação e uma regulação inteligente deve ter as seguintes características: baseada em princípios, com burocracia reduzida; apresentar baixo risco para o consumidor, evitando consentimentos desnecessários que geram fadiga para o consumidor; tecnologicamente neutra; leve, facilitando a transferência internacional, e; favorável ao investimento e à inovação, com ambiente de investimentos compatível com investimentos”. (p. 26). Todos disponíveis em: CÂMARA DOS DEPUTADOS. <https://www.camara.leg.br/proposicoesWeb/proprostrarintegra?codteor=1663305&filename=Tramitacao-PL%204060/2012>. Acesso em: 08 ago. 2023.

²⁹⁰ Nesse sentido a manifestação de Joana Varon, da *Coding Rights*, ao salientar que “a necessidade do “consentimento forte” e de autoridade para remediar e sancionar. Alertou para a perda de liberdade e o monopólio na internet na forma de “colonialismo digital”, salientando, como exemplos, a força dos data brokers (empresas que comercializam dados pessoais), ações do Google para permitir a cobrança no uso de bloqueadores de propagandas e do Facebook, que se utiliza dos microfones dos telefones de seus usuários”. (p. 20). CÂMARA DOS DEPUTADOS. Disponível em:

Segundo o relator, em alguma medida, todas essas contribuições e debates foram valiosos para o processo legislativo e ajudaram a moldar o texto final da Lei Geral de Proteção de Dados no Brasil. A diversidade de perspectivas e o engajamento de diferentes setores da sociedade contribuíram, conforme seu juízo, para a criação de uma legislação mais equilibrada e adequada à realidade brasileira.

Ao promover o encaminhamento, a Relatoria do PL não deixou de mencionar os riscos e efeitos que o atual estágio de desenvolvimento e emprego das ferramentas tecnológicas apresentam à sociedade, em razão da extraordinária capacidade de captura e tratamento de dados pessoais.

No entanto, consoante sobredito, mesmo para o Relator a preocupação principal, condutora da aprovação da legislação brasileira, com redação manifestamente similar à do RGPD²⁹¹, foi a de ver o país aberto aos interesses econômicos estrangeiros – algo que se mostra clarividente ao se visitar, *ipsis literis*, a justificativa por ele empregado, ao afirmar que “ao se viver nesta era em que dados e informações se tornaram insumos de negócios e movimentam vigorosíssimas indústrias globais, é extremamente necessário tornar o Brasil um ambiente integrado com o mundo e, portanto, propício para o desenvolvimento do setor” (Ibidem, p. 30).

O que se verifica do texto normativo ao final aprovado, portanto, é que os temas que envolveram os debates e contribuições não foram equanimemente contemplados no parecer – o que impactou na redação final do texto normativo da LGPD. As contribuições diversificadas não só enriqueceram os debates, mas também sublinharam a necessidade de adaptar a LGPD às demandas locais – aspectos praticamente esquecidos no afã de se estabelecer uma escoreta relação com o RGPD, e *um ambiente integrado com o mundo e, portanto, propício para o desenvolvimento do setor*²⁹².

https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=Tramitacao-PL%204060/2012. Acesso em: 08 ago. 2023.

²⁹¹ Ainda sobre o aspecto da similitude entre os textos normativos, rememora-se trabalho publicado pelo próprio autor:

²⁹² Sobre os interesses de que a legislação doméstica se adequasse às demandas econômicas e mercadológicas dos países de centro, já havia indicado o relator, no início de seu parecer: “Esse ponto, de a legislação do país estar de acordo com a legislação europeia, é extremamente pertinente neste julgamento, pois indica, como questão de fundo, a atratividade comercial do setor de TIC (Tecnologia da Informação e das Comunicações) dos países. Em tempos de computação em nuvem, um país que atenda à legislação europeia possui condições de atrair processamento de dados daquele bloco. E atrair o tratamento de dados implica não só a possibilidade de instalação de data centers, mas das próprias empresas de TIC, incluindo as gigantes ponto com. Por isso, a necessidade de o Brasil possuir,

A LGPD representa, portanto, uma tentativa clara de posicionar o Brasil em conformidade com as diretrizes europeias, em prol de relações comerciais e econômicas mais sólidas²⁹³. No entanto, a questão central que permanece é se essa abordagem de harmonização é suficiente para atender às nuances e complexidades específicas do Brasil e da América Latina. O equilíbrio entre a busca pela compatibilização e a proteção dos interesses regionais é um desafio contínuo que a LGPD enfrentará – ou, como é mais provável, desafio à frente do qual a LGPD *falhará*, consoante se percebe da postura adotada pela ANPD quando da aprovação da Resolução CD/ANPD nº 19/2024, com o objetivo de disciplinar o contido no capítulo V da Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018), acerca da transferência internacional de dados pessoais, compreendendo, em referido capítulo, a redação do art. 33 ao art. 36 da LGPD.

Ante o exposto, é inegável que a LGPD passou pelo regular processo legislativo, ingressando no mundo normativo dotada da correspondente presunção de validade. Sua característica de norma geral e abstrata, destinada a proteger as informações relacionadas à pessoa natural identificada ou identificável²⁹⁴, confere a seu texto a condição de matéria-prima a ser interpretada pelo jurista, a fim de dela extrair regras e princípios concernentes à matéria que almeja regular. Não há qualquer objeção a essa percepção, pautada, inclusive, na melhor compreensão do que significa o fenômeno jurídico-normativo, em uma perspectiva positivista do Direito²⁹⁵.

O reconhecimento desse aspecto não impede, no entanto, consoante argumentado outrora, que se promovam as críticas que ora se dirigem ao texto

sem abrir mão de suas especificidades e soberania, uma legislação harmônica com o mundo e com os principais blocos organizados, como a União Europeia”. *Ibidem*, p. 11.

²⁹³ Ao redigir seu encaminhamento, foi novamente enfático sobre a necessidade de adequação da LGPD às exigências nortecêntricas: “Por esse motivo e como discutido anteriormente, a não proteção aos dados pessoais, pode alijar o país de importantes oportunidades de desenvolvimento econômico”. *Ibidem*, p. 30.

²⁹⁴ Exclui-se do alcance normativo, conforme dita o art. 4º da LGPD, o tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

²⁹⁵ E, em razão disso, *formal*, enquanto condição *necessária* e *suficiente* para a formação de uma ordem jurídica, recuperando o que já exposto alhures a partir de Bobbio.

normativo: a excessiva reprodução dos ditames europeus, com preocupação diminuída acerca das especificidades do Brasil enquanto país consumidor de tecnologia leve e pesada capaz de capturar e tratar dados pessoais.

A fim de deixar absolutamente claro o que se afirma – ou seja, a similitude entre os textos, com o objetivo mais ou menos sub-reptício de se atender os interesses econômicos, políticos e culturais alienígenas em relação aos dados pessoais produzidos por nacionais e levados ao estrangeiro – é que se passa à análise da semelhança entre os textos da LGPD e do RGPD, no que diz respeito à transferência internacional de dados pessoais.

4.4 Uma comparação entre os textos normativos da LGPD e do RGPD: aspectos gerais

A análise comparativa responsável entre modelos jurídicos não pode se dar, simplesmente, ao talante do intérprete. Exige, em verdade, clareza metodológica. Por essa razão é que se adota o método funcional de direito comparado, na forma desenvolvida por Zweigert e Kötz, apresentado por Paula Maria Nasser Cury (CURY, 2014, p. 178). Procura-se, desse modo, respeitar o núcleo desse método, que pressupõe a compatibilidade do que se compara, isto é, de elementos que preenchem as mesmas funções jurídicas. No caso, diante da franca similaridade entre os textos normativos e os objetivos a que ambos se propõem, tanto as disposições constantes no ordenamento brasileiro quanto no europeu parecem objetos destinados a desempenhar funções similares. Desse modo, apontando-se, para cada um dos razão pela qual, presumindo-se a similitude, ciente de que a função cumpre o papel de elemento externo, e pretendendo-se a neutralidade na análise, permite-se a comparação dos direitos, valorando-se, no fim, os resultados obtidos (CURY, 2014, p. 179).

No subcapítulo anterior, nosso maior interesse foi o de verificar em que medida o trâmite legislativo responsável pela elaboração da normativa foi influenciado pelo arcabouço e nível de desenvolvimento europeu, razão pela qual não nos dedicamos à análise do texto da Lei Geral de Proteção de Dados (LGPD); no presente momento, no entanto, nos interessa cuidar do fato de se o texto normativo da lei

brasileira efetivamente tenta replicar o utilizado na redação da lei europeia, no que diz respeito à transferência internacional de dados pessoais. E, com maior especificidade, como a interpretação conferida ao texto doméstico reforça a posição submissa do país em sua condição subalterna no âmbito do fenômeno conhecido como *colonialismo de dados*.

A análise simultânea e comparativa dos ordenamentos brasileiro e europeu se justifica muito em razão da similaridade existente entre seus textos. Tal similitude, conforme antevisto, não é acidental, mas deriva da exigência europeia de que um país terceiro ou um organismo internacional assegure um nível de proteção adequado, ou seja, compatível com aquele que é conferido pelo regulamento europeu, a fim de que a transferência de dados pessoais ocorra de maneira legítima²⁹⁶. Tal juízo de adequação é emitido pela Comissão da União Europeia, com base em critérios dito objetivos, previstos no regulamento. No entanto, referido reconhecimento é realizado, unilateralmente, pela Comissão, o que demonstra a força cogente da União Europeia sobre os demais países na adoção, por estes, de medidas protetivas de dados pessoais aos moldes europeus.

No Brasil, por sua vez, a potencial capacidade nacional de exigir que um país terceiro ou um organismo internacional assegure um nível de proteção adequado ao brasileiro – ou seja, compatível com aquele que é conferido pela LGPD, e, quiçá, com uma futura legislação que se afirme como resposta contundente ao neoliberalismo e ao *colonialismo de dados*, a fim de que a transferência de dados pessoais ocorra de maneira legítima – mostra-se esvaziada, já que a própria Autoridade Nacional de Proteção de Dados se desobriga, de forma voluntário, de seu dever de emitir “decisões de adequação”, ao pretensamente regular o que dispõe sobre o assunto a LGPD.

Faremos a análise a partir de determinados excertos dos textos normativos²⁹⁷, selecionando, para tanto, seções e artigos de ambas as legislações, ínsitos ou correlatos ao tema ora em análise: a transferência internacional de dados pessoais.

²⁹⁶ Sobre o assunto, ainda, VIOLA, 2019.

²⁹⁷ A LGPD e o RGPD, a par das intensas similitudes, apresentam também algumas diferenças, que, apesar de não negligenciadas, não são capazes de convencer de que a Lei brasileira não foi editada para aplacar o desejo por adequação manifestado pela União Europeia. Por exemplo, no RGPD, a relação entre controlador e operador precisa ser formalizada, enquanto na LGPD o operador pode seguir as instruções do controlador sem um vínculo explícito. O RGPD impõe um prazo rigoroso de 72

Nesse sentido, o art. 3º da Lei Geral de Proteção de Dados (LGPD)²⁹⁸ e o art. 2º e 3º do Regulamento Geral de Proteção de Dados (RGPD)²⁹⁹ compartilham algumas semelhanças importantes em relação ao seu escopo de aplicação. A LGPD

horas para notificar violações de dados, enquanto a LGPD não especifica um prazo, definindo-o como razoável (art. 48, §1º). Quanto às penalidades, a GDPR prevê multas substancialmente maiores e medidas mais abrangentes, como advertências, bloqueio ou eliminação de dados e a suspensão de bancos de dados infratores. Essas são algumas amostras das diferenças entre os textos – incapazes, no entanto, de alterar a conclusão exarada acima.

²⁹⁸ Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019)

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Exceção-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

²⁹⁹ Artigo 2º -Âmbito de aplicação material

1. O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados.

2. O presente regulamento não se aplica ao tratamento de dados pessoais:

a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União;

b) Efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do TUE;

c) Efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas;

d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.

3. O Regulamento (CE) n.º 45/2001 aplica-se ao tratamento de dados pessoais pelas instituições, órgãos, organismos ou agências da União. O Regulamento (CE) n.º 45/2001, bem como outros atos jurídicos da União aplicáveis ao tratamento de dados pessoais, são adaptados aos princípios e regras do presente regulamento nos termos previstos no artigo 98.º.

4. O presente regulamento não prejudica a aplicação da Diretiva 2000/31/CE, nomeadamente as normas em matéria de responsabilidade dos prestadores intermediários de serviços previstas nos seus artigos 12.º a 15.º.

Artigo 3º - Âmbito de aplicação territorial

1. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União.

2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:

a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento;

b) O controle do seu comportamento, desde que esse comportamento tenha lugar na União.

3. O presente regulamento aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público.

se aplica a qualquer operação de tratamento de dados pessoais realizada no Brasil, bem como aquelas que tenham por objetivo a oferta de bens ou serviços a indivíduos localizados no território nacional e quando os dados pessoais forem coletados no Brasil. Por sua vez, o RGPD se aplica ao tratamento de dados pessoais, automatizados ou não, e é relevante tanto para entidades estabelecidas na União Europeia como para aquelas de fora da UE que ofereçam bens ou serviços a residentes da UE ou monitorem o comportamento dessas pessoas na UE.

Uma similitude significativa entre esses regulamentos é a aplicação extraterritorial. Ambos regulamentam o tratamento de dados pessoais não apenas dentro de seus territórios, mas também quando o tratamento tem impacto sobre os cidadãos de seu território. Isso significa que empresas e organizações de todo o mundo podem estar sujeitas a essas leis se lidarem com dados pessoais de cidadãos brasileiros (no caso da LGPD) ou de cidadãos da União Europeia (no caso do RGPD), mesmo que não estejam fisicamente localizadas nesses territórios.

Ambos os regulamentos, portanto, compartilham do entendimento de uma abordagem material e territorial ampla – se assim não fosse, dificilmente poderia o Brasil almejar a competente decisão de adequação europeia, já que teria seu âmbito de proteção diminuído e, potencialmente, entendido pela Comissão Europeia como insuficiente. Em nova comparação, quanto aos requisitos para o lícito tratamento de

dados pessoais, tanto o Artigo 6º do RGPD³⁰⁰ quanto o Artigo 7º da LGPD³⁰¹ estabelecem as bases legais para o tratamento de dados pessoais em suas

³⁰⁰ Artigo 6.º - Licitude do tratamento.

1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:

- a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
- b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
- c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
- d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
- e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
- f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica.

2. Os Estados-Membros podem manter ou aprovar disposições mais específicas com o objetivo de adaptar a aplicação das regras do presente regulamento no que diz respeito ao tratamento de dados para o cumprimento do n.º 1, alíneas c) e e), determinando, de forma mais precisa, requisitos específicos para o tratamento e outras medidas destinadas a garantir a licitude e lealdade do tratamento, inclusive para outras situações específicas de tratamento em conformidade com o capítulo IX.

3. O fundamento jurídico para o tratamento referido no n.º 1, alíneas c) e e), é definido:

- a) Pelo direito da União; ou
- b) Pelo direito do Estado-Membro ao qual o responsável pelo tratamento está sujeito.

A finalidade do tratamento é determinada com esse fundamento jurídico ou, no que respeita ao tratamento referido no n.º 1, alínea e), deve ser necessária ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento. Esse fundamento jurídico pode prever disposições específicas para adaptar a aplicação das regras do presente regulamento, nomeadamente: as condições gerais de licitude do tratamento pelo responsável pelo seu tratamento; os tipos de dados objeto de tratamento; os titulares dos dados em questão; as entidades a que os dados pessoais poderão ser comunicados e para que efeitos; os limites a que as finalidades do tratamento devem obedecer; os prazos de conservação; e as operações e procedimentos de tratamento, incluindo as medidas destinadas a garantir a legalidade e lealdade do tratamento, como as medidas relativas a outras situações específicas de tratamento em conformidade com o capítulo IX. O direito da União ou do Estado-Membro deve responder a um objetivo de interesse público e ser proporcional ao objetivo legítimo prosseguido.

4. Quando o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados ou em disposições do direito da União ou dos Estados-Membros que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no artigo 23.º, n.º 1, o responsável pelo tratamento, a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, tem nomeadamente em conta:

- a) Qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;
- b) O contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento;
- c) A natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 9º, ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10.º;
- d) As eventuais consequências do tratamento posterior pretendido para os titulares dos dados;

respectivas jurisdições. Ambos os artigos enfatizam a importância do consentimento do titular dos dados como uma base legal para o tratamento. Além disso, eles reconhecem a necessidade de cumprir obrigações legais e regulatórias como outra base para o tratamento de dados pessoais. Ambos os regulamentos também consideram o tratamento de dados pessoais no contexto de interesses legítimos. No RGPD, isso é detalhado no ponto (f) do art. 6º, enquanto na LGPD, é mencionado no inciso IX do art. 7º. Em ambos os casos, a proteção dos direitos e liberdades fundamentais dos titulares de dados é priorizada e deve ser equilibrada com os interesses legítimos do controlador ou de terceiros.

e) A existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização.

³⁰¹ Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019).

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

§ 1º (Revogado). (Redação dada pela Lei nº 13.853, de 2019).

§ 2º (Revogado). (Redação dada pela Lei nº 13.853, de 2019).

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019).

Tanto o RGPD quanto a LGPD estabelecem, portanto, as bases para o tratamento de dados de acordo com as obrigações legais, contratuais e legítimas. Pequenas diferenças podem ser observadas na terminologia utilizada em cada regulamento; no entanto, ambos enfatizam a necessidade de proteger os interesses vitais dos cidadãos, equilibrados com o interesse público – ou seja, legitimando o tratamento desde que respeite os direitos e liberdades fundamentais dos titulares de dados.

No que tange aos direitos dos titulares de dados pessoais, tanto a Lei Geral de Proteção de Dados quanto o Regulamento Geral de Proteção de Dados abordam essas questões de maneira mais detalhada em seus respectivos capítulos III, com ênfase especial nos artigos 18 da LGPD e 12º, 13º, 14º e 15º, do RGPD³⁰².

A legislação brasileira, especificamente no art. 18, estabelece o direito à confirmação e acesso, garantindo que qualquer pessoa natural tem o direito de confirmar se seus dados pessoais estão sendo processados e de obter acesso a essas informações. Além disso, esse texto confere aos titulares dos dados o direito de solicitar a correção de informações imprecisas, incompletas ou desatualizadas, bem como a possibilidade de revogar o consentimento previamente concedido. Adicionalmente, são previstas as prerrogativas de anonimização, bloqueio ou exclusão de dados.

No contexto do RGPD, o art. 12º enfatiza a transparência das informações e o direito de acesso, exigindo que os controladores forneçam informações de maneira clara, concisa e transparente aos titulares de dados, especialmente quando as informações se destinam a crianças. O RGPD também estabelece, em seu art. 15º, o direito do titular de obter informações detalhadas sobre o tratamento de seus dados, reforçando o acesso às informações pessoais e detalhes sobre o processamento.

Por sua vez, o art. 13º do RGPD requer que os controladores forneçam informações específicas aos titulares, incluindo a identificação do controlador e as finalidades do tratamento. Além disso, o art. 14º do RGPD consagra o direito do titular de solicitar ao controlador o acesso às informações pessoais relacionadas a si, a

³⁰² Ante a extensão dos textos normativos, remete-se à consulta aos documentos originais. Para verificação do contido na LGPD: BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 ago. 2023. Para consulta ao texto do RGPD: EUROPEAN UNION. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 15 ago. 2023.

possibilidade de corrigi-las, excluí-las ou restringir seu uso, bem como o direito de se opor ao processamento.

Ambas as leis, a LGPD brasileira e o RGPD europeu, portanto, compartilham, em seus textos, o direito dos titulares à transparência e ao acesso aos seus respectivos dados pessoais. Elas asseguram que os titulares de dados tenham a capacidade de confirmar, acessar e, se necessário, corrigir, anonimizar, bloquear ou eliminar seus dados pessoais. Ambas as regulamentações também reconhecem o direito dos titulares de dados de receber informações sobre como seus dados são compartilhados com terceiros. Além disso, ambas as leis estabelecem salvaguardas para proteger os titulares de dados contra decisões automatizadas que afetem seus interesses. Elas fornecem um mecanismo para revisão dessas decisões, incluindo o direito de saber os critérios utilizados³⁰³.

Embora haja, também nesse caso, diferenças nas redações e na organização dos artigos, os princípios subjacentes de proteção dos direitos dos titulares de dados são consistentes entre a LGPD brasileira e o RGPD europeu. Ambas as regulamentações têm como objetivo comum garantir a privacidade e a segurança dos dados pessoais, promovendo a transparência e o controle por parte dos titulares – ou, ao menos, anunciando a promoção dessa transparência e controle, a fim de satisfazer as exigências alienígenas, mais do que efetivamente as implementando, no caso da legislação nacional, para a tutela efetiva da maior parte dos cidadãos brasileiros.

A comparação entre os textos até o momento realizada demonstra, *mutatis mutandis*, o desejo de a legislação doméstica satisfazer o contido no Regulamento europeu. Ainda com esse desiderato, o último dos textos normativos a serem comparados corresponde, justamente, às previsões do RGPD e da LGPD destinadas a regulamentar a transferência internacional de dados pessoais, e, com mais especificidade ainda, a regulamentação das “decisões de adequação”.

³⁰³ Nesse sentido, os art. 20 da LGPD e art. 22 do RGPD. Sobre o assunto, ver: <https://techcompliance.org/decisoes-automatizadas/>. Acesso em: 15 ago. 2023.

4.5 A “decisão de adequação” no direito brasileiro e europeu

O Parlamento Europeu e o Conselho da União Europeia foram responsáveis pela edição do Regulamento 679/2016, 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. Referido regulamento teve sua aplicação iniciada em 25 de maio de 2018³⁰⁴, substituindo a Diretiva 95/46/CE, que correspondia, até então, ao Regulamento Geral sobre a Proteção de Dados.

Ao justificar a edição de uma nova normativa para proteção dos dados, o Parlamento Europeu e o Conselho da União Europeia indicaram que a anterior, constituída na forma de Diretiva, não se mostrava suficiente para tutelar os habitantes de seus Estados-membros, mormente ante os diferentes níveis de internalização do regramento, não adotado em plenitude por todos os Países, e o poderio de captação e tratamento de dados admitido pelas novas tecnologias. Desse modo, optou-se pela redação de um novo texto normativo, constituído na forma de Regulamento, cujo nível de vinculação e aplicação é superior ao da Diretiva³⁰⁵.

Ademais, embora a *Convenção 108*³⁰⁶ aborde, de forma abrangente, a proteção de dados e a necessidade de salvaguardas em transferências transfronteiriças, ela funciona como um tratado internacional que define princípios, e

³⁰⁴ Consoante o art. 99º do RGPD, *in verbis*:

Artigo 99.º

Entrada em vigor e aplicação

1. O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no Jornal Oficial da União Europeia.

2. O presente regulamento é aplicável a partir de 25 de maio de 2018.

³⁰⁵ Nesse sentido, a explicação apresentada pela própria União Europeia, por meio de informação contida em seu sítio eletrônico: Para alcançar os objetivos estabelecidos nos Tratados, a UE adota diferentes tipos de atos legislativos. Alguns desses atos são vinculativos, outros não. Alguns são aplicáveis a todos os países da UE, outros apenas a alguns deles. Regulamentos - Um «regulamento» é um ato legislativo vinculativo, aplicável em todos os seus elementos em todos os países da UE. Por exemplo, quando a UE quis garantir a aplicação de medidas comuns de salvaguarda aos produtos importados de fora da UE, o Conselho adotou um regulamento. (...) Diretivas - Uma «diretiva» é um ato legislativo que fixa um objetivo geral que todos os países da UE devem alcançar. Contudo, cabe a cada país elaborar a sua própria legislação para dar cumprimento a esse objetivo. É disso exemplo a Diretiva sobre direitos dos consumidores, que reforça esses direitos em toda a UE através designadamente da eliminação de encargos e custos ocultos na Internet e da extensão do período de que os consumidores dispõem para se retirar de um contrato de venda. Disponível em: https://europa.eu/european-union/eu-law/legal-acts_pt. Acesso em: 16 jul. 2024.

³⁰⁶ Disponível em: <https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2>. Acesso em 15 ago. 2023.

não uma regulamentação direta ou uniformemente aplicável dentro da União Europeia. A Convenção estabelece padrões mínimos de proteção e fomenta a cooperação internacional, mas não oferece o mesmo grau de detalhamento e exigências vinculativas que um regulamento como o RGPD³⁰⁷.

A exposição de motivos do Regulamento 679/2016, redigida na forma de *Considerandos*, deixa claro os objetivos da nova normativa: o incremento do nível de proteção aos dados pessoais³⁰⁸. As notas explicativas explicitam, ainda, o interesse

³⁰⁷ A *Convenção 108*, ou *Convenção para a Proteção das Pessoas em Relação ao Tratamento Automatizado de Dados de Caráter Pessoal*, adotada pelo Conselho da Europa em 1981, representa o primeiro tratado internacional vinculante sobre proteção de dados pessoais. Sua importância histórica e normativa é significativa, pois estabeleceu, já no início da era digital, um conjunto de princípios destinados a proteger a privacidade das pessoas contra o uso indevido de seus dados pessoais por meio de tecnologias automatizadas. A Convenção 108 é especialmente notável por seu alcance global: ela não se limita aos países membros do Conselho da Europa, mas também permite que países não europeus a ratifiquem, criando, assim, um padrão internacional de proteção de dados. A Convenção articula normas fundamentais para a proteção dos direitos dos indivíduos em relação aos dados pessoais, tais como a limitação de finalidade, a minimização de dados, a segurança e a transparência no tratamento. Esses princípios visam assegurar que os dados pessoais sejam coletados e processados de maneira justa e lícita e que sejam protegidos contra uso não autorizado ou ilegal, independentemente das fronteiras nacionais. Com a entrada em vigor do Protocolo Adicional em 2001, a Convenção 108 passou a incluir exigências específicas para a transferência internacional de dados pessoais, estabelecendo a necessidade de proteção adequada quando os dados são transferidos para jurisdições externas. Este Protocolo também reforça a obrigatoriedade de supervisão por autoridades independentes, que monitoram e aplicam as normas de proteção de dados dentro de cada país signatário. No contexto das transferências internacionais de dados pessoais, a Convenção 108 impacta diretamente a forma como os países signatários gerenciam as exportações de dados para países terceiros. Ela impõe a obrigação de garantir que as informações pessoais transferidas para fora das fronteiras dos países signatários sejam protegidas por padrões equivalentes aos estabelecidos na Convenção, seja por meio de legislação nacional, de decisões de adequação ou de cláusulas contratuais. Assim, a Convenção 108 promove um nível mínimo de proteção, independentemente do regime jurídico de proteção de dados de cada país receptor, limitando as disparidades e prevenindo potenciais riscos à privacidade dos indivíduos no âmbito internacional. A renovação da Convenção 108, conhecida como a "Convenção 108+", reforçou ainda mais esses princípios, alinhando-os ao cenário digital moderno e às demandas da proteção de dados na era da internet. Entre as atualizações introduzidas pela 108+, estão o fortalecimento dos direitos dos titulares dos dados, como o direito de não estar sujeito a decisões automatizadas e a obrigação dos países signatários de notificar violações de dados às autoridades competentes. A Convenção 108+, portanto, converte-se em uma ferramenta essencial para alinhar as práticas de proteção de dados entre diferentes regimes regulatórios, inclusive com o RGPD da União Europeia, e para consolidar um padrão global de proteção que apoie a continuidade dos direitos de privacidade além das fronteiras nacionais. Nesse sentido: Manual da legislação europeia sobre proteção de dados. 2014. 212 p. Disponível em: <https://rm.coe.int/16806ae65f>. Acesso em 16 ago. 2023.

³⁰⁸ Nesse sentido os considerandos nº 9, 10 e 11, assim redigidos: (9) Os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, mas não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros, podem impedir a livre circulação de dados pessoais na União. Essas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades económicas a nível da União, distorcer a concorrência e impedir as autoridades de

do Regulamento em normatizar a questão que impede o tráfego internacional de dados pessoais com países e organizações não dotados de sistema protetivo *de acordo* com o da União Europeia – não permitindo, portanto, o endereçamento e a circulação de dados pessoais a quaisquer ambientes e destinatários.

O Regulamento Geral de Proteção de Dados dedica um capítulo inteiro – Capítulo V – e mais de uma dezena de *considerandos* – Considerandos 101 a 116 – voltados à regulamentação das transferências internacionais de dados pessoais, *in casu*, para ambientes externos à União Europeia.

Os considerandos 101 a 116 do RGPD destacam a complexidade e a necessidade de regulamentação específica para transferências internacionais de dados pessoais entre a União Europeia (UE) e países terceiros ou organizações internacionais. O RGPD enfatiza que, embora a circulação de dados pessoais seja fundamental para o comércio e a cooperação global, ela deve preservar o alto padrão de proteção de dados garantido pela legislação europeia. O princípio orientador aqui é o de que os dados, mesmo fora das fronteiras da UE, devem ser tratados de acordo com normas equivalentes às europeias.

cumprirem as obrigações que lhes incumbem por força do direito da União. Essas diferenças e (10) A fim de assegurar um nível de proteção coerente e elevado das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais na União, o nível de proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento desses dados deverá ser equivalente em todos os Estados-Membros. É conveniente assegurar em toda a União a aplicação coerente e homogênea das regras de defesa dos direitos e das liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento de dados pessoais. No que diz respeito ao tratamento de dados pessoais para cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, os Estados-Membros deverão poder manter ou aprovar disposições nacionais para especificar a aplicação das regras do presente regulamento. Em conjugação com a legislação geral e horizontal sobre proteção de dados que dá aplicação à Diretiva 95/46/CE, os Estados-Membros dispõem de várias leis setoriais em domínios que necessitam de disposições mais específicas. O presente regulamento também dá aos Estados-Membros margem de manobra para especificarem as suas regras, inclusive em matéria de tratamento de categorias especiais de dados pessoais («dados sensíveis»). Nessa medida, o presente regulamento não exclui o direito dos Estados-Membros que define as circunstâncias de situações específicas de tratamento, incluindo a determinação mais precisa das condições em que é lícito o tratamento de dados pessoais.

(11) A proteção eficaz dos dados pessoais na União exige o reforço e a especificação dos direitos dos titulares dos dados e as obrigações dos responsáveis pelo tratamento e pela definição do tratamento dos dados pessoais, bem como poderes equivalentes para controlar e assegurar a conformidade das regras de proteção dos dados pessoais e sanções equivalentes para as infrações nos Estados-Membros. Disponível em: https://europa.eu/european-union/eu-law/legal-acts_pt. Acesso em: 16 jul. 2024.

Primeiramente, os considerandos afirmam que a Comissão Europeia tem a competência para decidir se um país terceiro ou uma organização internacional assegura um nível de proteção adequado (Considerando 10³⁰⁹). Este reconhecimento facilita a transferência de dados, dispensando autorizações adicionais, mas pode ser revogado se o país ou a organização não mantiver os padrões exigidos pela UE. A análise da Comissão deve, portanto, levar em conta aspectos como o respeito ao Estado de Direito e a adesão a normas internacionais de Direitos Humanos, conforme os valores fundamentais da União (Considerando 104³¹⁰). Esse nível de adequação é monitorado e revisado periodicamente, com consultas ao Parlamento Europeu e a outros órgãos (Considerando 106³¹¹).

³⁰⁹ (103) A Comissão pode decidir, com efeitos no conjunto da União, que um país terceiro, um território ou um setor determinado de um país terceiro, ou uma organização internacional, oferece um nível adequado de proteção de dados adequado, garantindo assim a segurança jurídica e a uniformidade ao nível da União relativamente ao país terceiro ou à organização internacional que seja considerado apto a assegurar tal nível de proteção. Nestes casos, podem realizar-se transferências de dados pessoais para esse país ou organização internacional sem que para tal seja necessária mais nenhuma autorização. A Comissão pode igualmente decidir, após enviar ao país terceiro ou organização internacional uma notificação e uma declaração completa dos motivos, revogar essa decisão.

³¹⁰ (104) Em conformidade com os valores fundamentais em que a União assenta, particularmente a defesa dos direitos humanos, a Comissão deverá, na sua avaliação do país terceiro ou de um território ou setor específico de um país terceiro, ter em consideração em que medida esse país respeita o primado do Estado de direito, o acesso à justiça e as regras e normas internacionais no domínio dos direitos humanos e a sua legislação geral e setorial, nomeadamente a legislação relativa à segurança pública, à defesa e à segurança nacional, bem como a lei da ordem pública e a lei penal. A adoção de uma decisão de adequação relativamente a um território ou um setor específico num país terceiro deverá ter em conta critérios claros e objetivos, tais como as atividades de tratamento específicas e o âmbito das normas jurídicas aplicáveis, bem como a legislação em vigor no país terceiro. Este deverá dar garantias para assegurar um nível adequado de proteção essencialmente equivalente ao assegurado na União, nomeadamente quando os dados pessoais são tratados num ou mais setores específicos. Em especial, o país terceiro deverá garantir o controlo efetivo e independente da proteção dos dados e estabelecer regras de cooperação com as autoridades de proteção de dados dos Estados-Membros, e ainda conferir aos titulares dos dados direitos efetivos e oponíveis e vias efetivas de recurso administrativo e judicial.

³¹¹ (106) A Comissão deverá controlar a eficácia das decisões sobre o nível de proteção assegurado num país terceiro, num território ou num setor específico de um país terceiro, ou numa organização internacional, e acompanhar a eficácia das decisões adotadas com base no artigo 25.o, n.º 6, ou no artigo 26.o, n.º 4, da Diretiva 95/46/CE. Nas suas decisões de adequação, a Comissão deverá prever um procedimento de avaliação periódica da aplicação destas. Essa revisão periódica deverá ser feita em consulta com o país terceiro ou a organização internacional em questão e ter em conta todos os desenvolvimentos pertinentes verificados no país terceiro ou organização internacional. Para efeitos de controlo e de realização das revisões periódicas, a Comissão deverá ter em consideração os pontos de vista e as conclusões a que tenham chegado o Parlamento Europeu e o Conselho, bem como outros organismos e fontes pertinentes. A Comissão deverá avaliar, num prazo razoável, a eficácia destas últimas decisões e comunicar quaisquer resultados pertinentes ao comité na aceção do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho (12), tal como estabelecido no presente regulamento, ao Parlamento Europeu e ao Conselho.

Nos casos em que a Comissão não identificar a presença de uma proteção adequada, os responsáveis pelo tratamento de dados devem adotar garantias complementares, como cláusulas contratuais, regras vinculativas e outras salvaguardas para assegurar que os direitos dos titulares de dados sejam respeitados (Considerando 108³¹²). Essas garantias devem possibilitar o acesso a recursos administrativos e judiciais, tanto na União quanto em países terceiros, conforme o princípio de proteção de dados desde a concepção e por defeito.

Os considerandos ainda abordam a importância das derrogações³¹³ em transferências baseadas no consentimento do titular ou em interesses públicos importantes, como questões de saúde pública ou segurança (Considerandos 111-112³¹⁴). Para transferências que não atendam aos requisitos de adequação, o RGPD

³¹² (108) Na falta de uma decisão sobre o nível de proteção adequado, o responsável pelo tratamento ou o subcontratante deverá adotar as medidas necessárias para colmatar a insuficiência da proteção de dados no país terceiro dando para tal garantias adequadas ao titular dos dados. Tais garantias adequadas podem consistir no recurso a regras vinculativas aplicáveis às empresas, cláusulas-tipo de proteção de dados adotadas pela Comissão, cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo, ou cláusulas contratuais autorizadas por esta autoridade. Essas medidas deverão assegurar o cumprimento dos requisitos relativos à proteção de dados e o respeito pelos direitos dos titulares dos dados adequados ao tratamento no território da União, incluindo a existência de direitos do titular de dados e de medidas jurídicas corretivas eficazes, nomeadamente o direito de recurso administrativo ou judicial e de exigir indemnização, quer no território da União quer num país terceiro. Deverão estar relacionadas, em especial, com o respeito pelos princípios gerais relativos ao tratamento de dados pessoais e pelos princípios de proteção de dados desde a concepção e por defeito. Também podem ser efetuadas transferências por autoridades ou organismos públicos para autoridades ou organismos públicos em países terceiros ou para organizações internacionais que tenham deveres e funções correspondentes, nomeadamente com base em disposições a inserir no regime administrativo, como seja um memorando de entendimento, que prevejam a existência de direitos efetivos e oponíveis dos titulares dos dados. Deverá ser obtida a autorização da autoridade de controlo competente quando as garantias previstas em regimes administrativos não forem juridicamente vinculativas.

³¹³ As derrogações funcionam como exceções especiais para a transferência de dados pessoais para fora da União Europeia (UE), ou seja, para países ou organizações internacionais que não têm uma “decisão de adequação” da Comissão Europeia, que certifique que possuem um nível adequado de proteção de dados. Essas exceções são necessárias em situações específicas onde a transferência dos dados é crucial por algum motivo, e o RGPD permite essas derrogações para que os dados possam ser transferidos mesmo na ausência de um nível de proteção equivalente ao europeu. Tais situações específicas incluem: os casos em que a transferência se mostra essencial para o interesse público; quando se faz necessária para proteger vidas humanas ou sua integridade física; no âmbito de missões humanitárias em situações extremas, como conflitos armados.

³¹⁴ (111) Deverá prever-se a possibilidade de efetuar transferências em determinadas circunstâncias em que o titular dos dados dê o seu consentimento explícito, em que a transferência seja ocasional e necessária em relação a um contrato ou a um contencioso judicial, independentemente de se tratar de um processo judicial, de um processo administrativo ou de um qualquer procedimento não judicial, incluindo procedimentos junto de organismos de regulação. Deverá também estar prevista a possibilidade de efetuar transferências no caso de motivos importantes de interesse público previstos pelo direito da União ou de um Estado-Membro o exigirem, ou se a transferência for efetuada a partir de um registo criado por lei e destinado à consulta por parte do público ou de pessoas com um interesse legítimo. Neste último caso, a transferência não deverá abranger a totalidade dos dados nem categorias

permite transferências pontuais, desde que não afetem negativamente os direitos dos titulares dos dados (Considerando 113³¹⁵).

Finalmente, destaca-se que as transferências transfronteiriças impõem desafios adicionais ao exercício dos direitos de proteção de dados e ao monitoramento por autoridades de controle (Considerando 116³¹⁶). Para mitigar esses

completas de dados pessoais contidos nesse registo e, quando este último se destinar a ser consultado por pessoas com um interesse legítimo, a transferência apenas deverá ser *efetuada a pedido dessas pessoas ou, caso sejam os seus destinatários, tendo plenamente em conta* os interesses e os direitos fundamentais do titular dos dados. (112) Essas derrogações deverão ser aplicáveis, em especial, às transferências de dados exigidas e necessárias por razões importantes de interesse público, por exemplo em caso de intercâmbio internacional de dados entre autoridades de concorrência, administrações fiscais ou aduaneiras, entre autoridades de supervisão financeira, entre serviços competentes em matéria de segurança social ou de saúde pública, por exemplo em caso de localização de contactos no que respeita a doenças contagiosas ou para reduzir e/ou eliminar a dopagem no desporto. Deverá igualmente ser considerada legal uma transferência de dados pessoais que seja necessária para a proteção de um interesse essencial para os interesses vitais do titular dos dados ou de outra pessoa, nomeadamente a integridade física ou a vida, se o titular dos dados estiver impossibilitado de dar o seu consentimento. Na falta de uma decisão de adequação, o direito da União ou de um Estado-Membro pode, por razões importantes de interesse público, estabelecer expressamente limites à transferência de categorias específicas de dados para países terceiros ou organizações internacionais. Os Estados-Membros deverão notificar essas decisões nacionais à Comissão. As transferências, para uma organização humanitária internacional, de dados pessoais de um titular que seja física ou legalmente incapaz de dar o seu consentimento, com vista ao desempenho de missões, ao abrigo das Convenções de Genebra ou para cumprir o direito internacional humanitário aplicável aos conflitos armados, poderão ser consideradas necessárias por uma razão importante de interesse público ou por ser do interesse vital do titular dos dados.

³¹⁵ (113) As transferências que possam ser classificadas como não repetitivas e que apenas digam respeito a um número limitado de titulares de dados podem igualmente ser admitidas para efeitos dos interesses legítimos imperiosos visados pelo responsável pelo tratamento, desde que a tais interesses não se sobreponham os interesses ou os direitos e liberdades do titular dos dados e desde que o responsável pelo tratamento destes tenha avaliado todas as circunstâncias associadas à operação de transferência. O responsável pelo tratamento deverá atender especialmente à natureza dos dados pessoais, à finalidade e à duração da operação ou operações de tratamento previstas, bem como à situação vigente no país de origem, no país terceiro e no país de destino final, e deverá apresentar as garantias adequadas para defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento dos seus dados pessoais. Tais transferências só deverão ser possíveis em raros casos em que não se aplique nenhum dos outros motivos de transferência. Para fins de investigação científica ou histórica ou fins estatísticos, deverão ser tidas em consideração as expectativas legítimas da sociedade em matéria de avanço do conhecimento. O responsável pelo tratamento deverá informar da transferência a autoridade de controlo e o titular dos dados.

³¹⁶ (116) Sempre que dados pessoais atravessarem fronteiras fora do território da União, aumenta o risco de que as pessoas singulares não possam exercer os seus direitos à proteção de dados, nomeadamente para se protegerem da utilização ilegal ou da divulgação dessas informações. Paralelamente, as autoridades de controlo podem ser incapazes de dar seguimento a reclamações ou conduzir investigações relacionadas com atividades exercidas fora das suas fronteiras. Os seus esforços para colaborar no contexto transfronteiras podem ser também restringidos por poderes preventivos ou medidas de reparação insuficientes, regimes jurídicos incoerentes e obstáculos práticos, tais como a limitação de recursos. Por conseguinte, revela-se necessário promover uma cooperação mais estreita entre as autoridades de controlo da proteção de dados, a fim de que possam efetuar o intercâmbio de informações e realizar investigações com as suas homólogas internacionais. Para efeitos de criação de regras de cooperação internacional que facilitem e proporcionem assistência mútua internacional para a aplicação da legislação de proteção de dados pessoais, a Comissão e as autoridades de controlo deverão trocar informações e colaborar com as autoridades competentes de

desafios, o regulamento encoraja a cooperação internacional entre autoridades de proteção de dados, promovendo assistência mútua e a troca de informações com base na reciprocidade e no respeito às normas do RGPD. Esses mecanismos de cooperação visam assegurar que, mesmo além das fronteiras da UE, o direito à proteção de dados seja efetivamente mantido.

O Capítulo V do RGPD, por sua vez, aborda detalhadamente as condições e mecanismos para transferências de dados pessoais a países terceiros e organizações internacionais, enquanto resposta regulatória para assegurar a proteção de dados além das fronteiras da União Europeia. O princípio geral das transferências, exposto no Artigo 44^o, determina que qualquer transferência internacional de dados pessoais deve garantir que o nível de proteção não seja comprometido. Esse princípio reforça a premissa do regulamento, assegurando a continuidade da proteção de dados independentemente do destino³¹⁷. O Artigo 45.^o introduz a *decisão de adequação*³¹⁸,

países terceiros em atividades relacionadas com o exercício dos seus poderes, com base na reciprocidade e em conformidade com o presente regulamento.

³¹⁷ Artigo 44.^o Princípio geral das transferências: Qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional só é realizada se, sem prejuízo das outras disposições do presente regulamento, as condições estabelecidas no presente capítulo forem respeitadas pelo responsável pelo tratamento e pelo subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional. Todas as disposições do presente capítulo são aplicadas de forma a assegurar que não é comprometido o nível de proteção das pessoas singulares garantido pelo presente regulamento.

³¹⁸ Artigo 45.^o Transferências com base numa decisão de adequação

1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica.

2. Ao avaliar a adequação do nível de proteção, a Comissão tem nomeadamente em conta os seguintes elementos:

a) O primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais, a legislação pertinente em vigor, tanto a geral como a setorial, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais, bem como a aplicação dessa legislação e das regras de proteção de dados, das regras profissionais e das medidas de segurança, incluindo as regras para a transferência ulterior de dados pessoais para outro país terceiro ou organização internacional, que são cumpridas nesse país ou por essa organização internacional, e a jurisprudência, bem como os direitos dos titulares dos dados efetivos e oponíveis, e vias de recurso administrativo e judicial para os titulares de dados cujos dados pessoais sejam objeto de transferência;

b) A existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros; e

c) Os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional em causa, ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos,

que permite à Comissão Europeia autorizar transferências sem necessidade de autorizações específicas se considerar que um país terceiro ou organização internacional possui um nível de proteção de dados adequado. Esse processo envolve uma análise rigorosa dos aspectos institucionais e jurídicos do país, como o respeito ao Estado de Direito, proteção dos direitos humanos e existência de uma autoridade independente de proteção de dados. A decisão é revisada periodicamente, permitindo ajustes conforme mudanças no contexto do país ou organização.

Nos casos em que não há uma decisão de adequação, o Artigo 46.º estipula que os responsáveis pelo tratamento de dados devem implementar garantias adequadas, como cláusulas contratuais padrão, regras vinculativas de empresas ou acordos específicos entre autoridades públicas. Essas medidas, que buscam

bem como da sua participação em sistemas multilaterais ou regionais, em especial em relação à proteção de dados pessoais.

3. Após avaliar a adequação do nível de proteção, a Comissão pode decidir, através de um ato de execução, que um país terceiro, um território ou um ou mais setores específicos de um país terceiro, ou uma organização internacional, garante um nível de proteção adequado na aceção do n.º 2 do presente artigo. O ato de execução prevê um procedimento de avaliação periódica, no mínimo de quatro em quatro anos, que deverá ter em conta todos os desenvolvimentos pertinentes no país terceiro ou na organização internacional. O ato de execução especifica o âmbito de aplicação territorial e setorial e, se for caso disso, identifica a autoridade ou autoridades de controlo a que se refere o n.º 2, alínea b), do presente artigo. O referido ato de execução é adotado pelo procedimento de exame a que se refere o artigo 93.o, n.º 2.

4. A Comissão controla, de forma continuada, os desenvolvimentos nos países terceiros e nas organizações internacionais que possam afetar o funcionamento das decisões adotadas nos termos do n.º 3 do presente artigo e das decisões adotadas com base no artigo 25.o, n.o 6, da Diretiva 95/46/CE.

5. A Comissão, sempre que a informação disponível revelar, nomeadamente na sequência da revisão a que se refere o n.º 3 do presente artigo, que um país terceiro, um território ou um ou mais setores específicos de um país terceiro, ou uma organização internacional, deixou de assegurar um nível de proteção adequado na aceção do n.º 2 do presente artigo, na medida do necessário, revoga, altera ou suspende a decisão referida no n.º 3 do presente artigo, através de atos de execução, sem efeitos retroativos. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 93.o, n.º 2.

Por imperativos de urgência devidamente justificados, a Comissão adota atos de execução imediatamente aplicáveis pelo procedimento a que se refere o artigo 93.o, n.º 3.

6. A Comissão inicia consultas com o país terceiro ou a organização internacional com vista a corrigir a situação que tiver dado origem à decisão tomada nos termos do n.º 5.

7. As decisões tomadas ao abrigo do n.º 5 do presente artigo não prejudicam as transferências de dados pessoais para o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou para a organização internacional em causa, nos termos dos artigos 46.o a 49.o.

8. A Comissão publica no Jornal Oficial da União Europeia e no seu sítio web uma lista dos países terceiros, territórios e setores específicos de um país terceiro e de organizações internacionais relativamente aos quais tenha declarado, mediante decisão, se asseguram ou não um nível de proteção adequado.

9. As decisões adotadas pela Comissão com base no artigo 25.o, n.º 6, da Diretiva 95/46/CE permanecem em vigor até que sejam alteradas, substituídas ou revogadas por uma decisão da Comissão adotada em conformidade com o n.º 3 ou o n.º 5 do presente artigo.

assegurar os direitos dos titulares, tornam-se essenciais para manter a segurança jurídica e as garantias dos dados pessoais transferidos³¹⁹.

O Artigo 47.º detalha as regras vinculativas de empresas, aplicáveis a transferências intragrupo para países terceiros, exigindo que as organizações implementem mecanismos juridicamente vinculantes que garantam o respeito aos direitos dos titulares. Esse artigo especifica uma série de obrigações, como a criação de estruturas internas de monitoramento, comunicação com autoridades de proteção de dados e sistemas de treinamento e resposta a incidentes³²⁰.

No caso de decisões judiciais ou administrativas que exijam transferências, o Artigo 48.º estipula que elas só serão reconhecidas quando baseadas em acordos internacionais válidos entre a UE e o país terceiro, resguardando o RGPD de interferências externas³²¹.

O Artigo 49.º prevê derrogações específicas para situações excepcionais, permitindo transferências baseadas no consentimento do titular, por interesse público, ou para a proteção de direitos essenciais, quando inexistem decisões de adequação ou garantias adequadas³²².

³¹⁹ Artigo 46.º Transferências sujeitas a garantias adequadas

1. Não tendo sido tomada qualquer decisão nos termos do artigo 45.o, n.º 3, os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes.

(...)

³²⁰ Artigo 47.º Regras vinculativas aplicáveis às empresas:

1. Pelo procedimento de controlo da coerência previsto no artigo 63.o, a autoridade de controlo competente aprova regras vinculativas aplicáveis às empresas, que devem:

a) Ser juridicamente vinculativas e aplicáveis a todas as entidades em causa do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta, incluindo os seus funcionários, as quais deverão assegurar o seu cumprimento; b) Conferir expressamente aos titulares dos dados direitos oponíveis relativamente ao tratamento dos seus dados pessoais; e
c) Preencher os requisitos estabelecidos no n.º 2. (...)

³²¹ Artigo 48.º Transferências ou divulgações não autorizadas pelo direito da União

As decisões judiciais e as decisões de autoridades administrativas de um país terceiro que exijam que o responsável pelo tratamento ou o subcontratante transfiram ou divulguem dados pessoais só são reconhecidas ou executadas se tiverem como base um acordo internacional, como um acordo de assistência judiciária mútua, em vigor entre o país terceiro em causa e a União ou um dos Estados-Membros, sem prejuízo de outros motivos de transferência nos termos do presente capítulo.

³²² Artigo 49.º Derrogações para situações específicas

1. Na falta de uma decisão de adequação nos termos do artigo 45.º, n.º 3, ou de garantias adequadas nos termos do artigo 46.o, designadamente de regras vinculativas aplicáveis às empresas, as transferências ou conjunto de transferências de dados pessoais para países terceiros ou organizações internacionais só são efetuadas caso se verifique uma das seguintes condições:

(...)

Por fim, o Artigo 50.º promove a cooperação internacional, incentivando a Comissão e autoridades de controle a colaborarem com países terceiros para a aplicação efetiva da legislação de proteção de dados. Essa cooperação busca harmonizar práticas, facilitar a investigação e promover o compartilhamento de informações, visando à proteção global dos dados pessoais³²³.

Consoante se observa ao se analisar, portanto, tanto os *Considerandos* quanto os artigos ínsitos ao Capítulo V do RGPD, vê-se que a estrutura das transferências internacionais de dados no contexto europeu baseia-se, primordialmente, em duas abordagens regulamentares: a decisão de adequação e o uso de cláusulas contratuais, que buscam assegurar a proteção contínua e a segurança jurídica dos dados pessoais ao serem transferidos para fora do território da União Europeia.

A decisão de adequação, descrita, com mais ênfase, no Artigo 45º, consiste em uma medida regulatória pela qual a Comissão Europeia avalia se um país terceiro ou uma organização internacional oferece um nível de proteção de dados equivalente ao garantido dentro da União. Para que um país seja considerado "adequado," ele deve demonstrar um compromisso firme com os princípios de proteção de dados, incorporando, por exemplo, o respeito ao Estado de Direito, a proteção dos Direitos Humanos e a existência de uma autoridade independente que supervisiona a proteção de dados. Caso a Comissão identifique um nível de proteção adequado, as transferências de dados para esse país são automaticamente autorizadas e não requerem acordos adicionais, o que facilita o fluxo de dados ao mesmo tempo que preserva o nível de segurança exigido pela legislação europeia.

³²³ Artigo 50.º Cooperação internacional no domínio da proteção de dados pessoais

Em relação a países terceiros e a organizações internacionais, a Comissão e as autoridades de controlo tomam as medidas necessárias para:

- a) Estabelecer regras internacionais de cooperação destinadas a facilitar a aplicação efetiva da legislação em matéria de proteção de dados pessoais;
- b) Prestar assistência mútua a nível internacional no domínio da aplicação da legislação relativa à proteção de dados pessoais, nomeadamente através da notificação, comunicação de reclamações, e assistência na investigação e intercâmbio de informações, sob reserva das garantias adequadas de proteção dos dados pessoais e de outros direitos e liberdades fundamentais;
- c) Associar as partes interessadas aos debates e atividades que visem intensificar a cooperação internacional no âmbito da aplicação da legislação relativa à proteção de dados pessoais;
- d) Promover o intercâmbio e a documentação da legislação e das práticas em matéria de proteção de dados pessoais, nomeadamente no que diz respeito a conflitos jurisdicionais com países terceiros.

Por outro lado, as cláusulas contratuais padrão e outras formas de garantias contratuais, previstas no Artigo 46º, operam como uma alternativa quando a decisão de adequação não está presente. Essas cláusulas, desenvolvidas e aprovadas pela Comissão, funcionam como acordos jurídicos entre as partes que transferem e recebem os dados, impondo obrigações específicas e detalhadas para garantir que o tratamento dos dados ocorra de maneira compatível com o RGPD. As cláusulas contratuais estabelecem padrões de segurança e procedimentos para o tratamento de dados, oferecendo uma base segura para a transferência ao exigir que os dados sejam processados em conformidade com os princípios europeus de proteção de dados.

Além disso, as regras vinculativas de empresas (Artigo 47.º) são utilizadas para transferências dentro de grupos empresariais internacionais, garantindo que todas as entidades pertencentes ao mesmo grupo empresarial mantenham as mesmas normas de proteção de dados, independentemente da sua localização geográfica. Essas regras, que são juridicamente obrigatórias para todas as subsidiárias, refletem uma tentativa de uniformizar as práticas de proteção de dados, preservando a integridade dos dados pessoais e os direitos dos titulares, mesmo em ambientes extraterritoriais.

Esses mecanismos, somados às derrogações específicas para situações excepcionais (Artigo 49.º) e à cooperação internacional com autoridades de proteção de dados (Artigo 50.º), constituem um sistema amplo, que busca assegurar que os dados pessoais de cidadãos da União Europeia sejam tratados com um nível de segurança adequado, seja por meio de adequação regulatória ou de acordos contratuais.

Diante desse contexto, a fim de avaliar o grau de conformidade de cada nação, a Comissão Europeia, órgão responsável pela emissão das *decisões de adequação*, aprecia uma série de fatores. Isso inclui a legislação vigente, tanto de caráter geral quanto setorial, o compromisso com Direitos Humanos e liberdades fundamentais, bem como a presença e a eficácia operacional de uma ou mais autoridades independentes de proteção de dados³²⁴.

³²⁴ Sobre o assunto, assim expressamente se posiciona a Comissão Europeia:

“A Comissão Europeia tem competência para determinar, com base no artigo 45.º do Regulamento (UE) 2016/679, se um país fora da UE oferece um nível adequado de proteção de dados.

As decisões de adequação exercem influência na estrutura de governança e nas operações de entidades econômicas estrangeiras que desejam operar no mercado interno da União Europeia, ou que já estão atuando nele. Assim, essas entidades passam a aderir às decisões de adequação como um requisito para obter acesso ao mercado interno da União Europeia. Essas decisões têm, como finalidade precípua, buscar um equilíbrio entre a proteção dos investidores, a manutenção dos mercados financeiros da União Europeia abertos em escala global e a estabilidade financeira. Além disso, visam a promover a convergência regulatória e aprimorar a colaboração na supervisão com parceiros estrangeiros.

O posicionamento da União Europeia, que busca influenciar países terceiros a alinhar suas legislações com a legislação europeia, está em conformidade com o princípio orientador de sua atuação externa, conhecido como o *princípio da responsabilidade*. Esse princípio reflete um objetivo de longa data de seus órgãos, de aumentar a visibilidade e a eficácia de sua atuação internacional, com o intuito de se tornar uma potência capaz de exercer uma influência *ética* sobre a globalização (MESQUITA, 2011, p. 184). Abordando esse cenário, Abraham Newman e Eliot Posner (2015, p. 1316 e ss.) esclarecem que "as normas de equivalência incentivam empresas ativas internacionalmente a pressionar por reformas regulatórias em seus

A adoção de uma decisão de adequação implica:

- uma proposta da Comissão Europeia;
- um parecer do Comité Europeu para a Proteção de Dados;
- uma aprovação de representantes dos países da UE;
- adoção da decisão pela Comissão Europeia.

Em qualquer momento, o Parlamento Europeu e o Conselho podem solicitar à Comissão Europeia que mantenha, altere ou retire a decisão de adequação com o fundamento de que o seu ato excede as competências de execução previstas no regulamento.

O efeito de tal decisão é que os dados pessoais podem ser transferidos da UE (e da Noruega, do Listenstaine e da Islândia) para esse país terceiro sem que seja necessária qualquer outra salvaguarda. Por outras palavras, as transferências para o país em questão serão equiparadas às transmissões de dados intra-UE.

Até à data, a Comissão Europeia reconheceu Andorra, Argentina, Canadá (organizações comerciais), Ilhas Faroé, Guernsey, Israel, Ilha de Man, Japão, Jersey, Nova Zelândia, República da Coreia, Suíça, Reino Unido ao abrigo do RGPD e LED, os Estados Unidos (organizações comerciais que participam no Quadro de Privacidade de Dados UE-EUA) e Uruguai como proporcionando proteção adequada. Com exceção do Reino Unido, estas decisões de adequação não abrangem os intercâmbios de dados no setor da aplicação da lei que são regidos pela Diretiva relativa à aplicação da lei (artigo 36.º da Diretiva (UE) 2016/680)".

Disponível em: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_pt?ettrans=pt. Acesso em: 18 jul. 2024.

países de origem". Portanto, a União Europeia exerce influência nas reformas regulatórias em países terceiros, agindo como um promotor de normas.

Do panorama apresentado, depreende-se, portanto, que o Regulamento 679/2016 não apenas estabelece um robusto *framework* para a proteção de dados pessoais dentro da União Europeia, mas também se configura como um instrumento de influência regulatória global. Ao exigir que países terceiros atendam aos rigorosos padrões de proteção de dados europeus como condição para a transferência internacional de dados, a União Europeia não busca apenas garantir a segurança e privacidade de seus cidadãos, mas também promover uma harmonização global das práticas de proteção de dados. Esse movimento reforça, a um, a posição da União Europeia como líder em governança de dados e catalisador de mudanças regulatórias internacionais, incentivando a convergência de normas e a cooperação internacional em matéria de proteção de dados pessoais, e, a dois, seu protagonismo econômico e política, que se espalha em sua legislação protetiva de dados pessoais, com vistas não a assegurar o direito de toda a humanidade à proteção de dados, mas a de seus nacionais – o que se percebe ao se compulsar a literatura, justamente, sobre o poder da privacidade, o neoliberalismo e o colonialismo de dados.

Em decorrência do Regulamento Geral de Proteção de Dados Pessoais europeu e a previsão nele contida de se exigir de outros Estados um nível de proteção adequado, reconhecido mediante *decisões de adequação*, para a legítima transferência internacional de dados pessoais, o Brasil, de maneira expedita, tratou de editar uma legislação inspirada na europeia, precipuamente para que as relações comerciais que exijam o intercâmbio de dados pessoais entre os territórios possam ser regularmente mantidas³²⁵.

Nesse contexto é que foi aprovada, em 14 de agosto de 2018, no Brasil, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados, com entrada em vigor no mês de setembro de 2020. Em que pese derivada do Projeto de Lei nº 4.060,

³²⁵ Nesse sentido o contido no prefácio da obra "Lei Geral de Proteção de Dados Pessoais: comentada artigo por artigo", ao se afirmar que: quanto aos aspectos relacionados à circulação transfronteiriça dos dados pessoais, o modelo estabelecido na União Europeia é a partir do juízo de adequação. Em outras palavras, os dados pessoais de europeus somente podem ser enviados para países que tenham um nível adequado aos padrões europeus de proteção de dados pessoais. De sorte que o Brasil conta com uma lei de proteção de dados pessoais inspirada no modelo europeu, o que se concretizará com a criação da ANPD e sua implantação e atuação de maneira independente, o que colaborará positivamente para a inserção do Brasil no capitalismo informacional. (TEIXEIRA, 2019, p. 9).

de 2012, apenas em 22 de maio de 2018 – ou seja, três dias antes do início da eficácia da RGPD – é que recebeu, de seu relator, requerimento de urgência para tramitação³²⁶.

Até o final de outubro de 2024, o Brasil ainda não havia recebido o reconhecimento de “país adequado” por parte da Comissão Europeia. É importante destacar que, mesmo com o estabelecimento da Autoridade Nacional de Proteção de Dados (ANPD), a independência efetiva dessa autoridade figura como uma questão crítica para que o Brasil alcance tal reconhecimento³²⁷.

No âmbito da Lei Geral de Proteção de Dados brasileira, a regulamentação acerca da transferência internacional de dados ficou reservada – quis, quiçá, o destino, para as vozes que apregoam uma ausência de “submissão” da legislação brasileira à estrangeira – ao Capítulo V de referido diploma normativo.

O sistema de transferência internacional de dados pessoais na LGPD, exposto nos Artigos 33 a 36, estabelece as condições sob as quais esses dados podem ser enviados para outros países, objetivando a manutenção de um nível adequado de proteção conforme os princípios da LGPD. Inspirado nas diretrizes europeias, o Capítulo V da LGPD busca garantir que, mesmo fora do território nacional, os dados dos cidadãos brasileiros sejam tratados com padrões rigorosos de segurança e privacidade.

O Artigo 33 define as situações nas quais a transferência internacional é permitida³²⁸. Entre os cenários autorizados, destaca-se a transferência para países

³²⁶ Nesse sentido, a íntegra do requerimento: https://www.camara.leg.br/proposicoesWeb/prop_mostrarnetgra;jsessionid=7940B2663EF5BB140A428FF22B66F40F.proposicoesWebExterno2?codteor=1662254&filename=Tramitacao-PL+4060/2012. Acesso em: 19 jul. 2024.

³²⁷ Deve-se considerar, nesse sentido, que apenas no mês de outubro de 2022 a Autoridade Nacional de Proteção de Dados passou a gozar, após a promulgação da Lei nº 14.460/2022, responsável por transformar a ANPD em autarquia de natureza especial, de autonomia financeira e administrativa.

³²⁸ Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
a) cláusulas contratuais específicas para determinada transferência;
b) cláusulas-padrão contratuais;
c) normas corporativas globais;
d) selos, certificados e códigos de conduta regularmente emitidos;
III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

que ofereçam uma proteção considerada “adequada”, semelhante ao conceito de “decisão de adequação” do RGPD. Além disso, outras formas de autorização incluem garantias de proteção adicionais, como cláusulas contratuais específicas, normas corporativas globais e mecanismos de certificação, que obrigam o destinatário estrangeiro a respeitar os princípios da LGPD. Esse artigo também permite a transferência em casos de consentimento expreso do titular, necessidade de cooperação jurídica internacional e outras situações de interesse público e segurança.

O Artigo 34 atribui à Autoridade Nacional de Proteção de Dados (ANPD) a função de avaliar o nível de proteção dos países estrangeiros, considerando critérios como a legislação do país receptor, a natureza dos dados transferidos, às garantias judiciais e institucionais, e as medidas de segurança implementadas³²⁹. Esse papel da ANPD é crucial, pois permite que o Brasil exerça controle sobre a adequação dos países terceiros, criando uma barreira regulatória que busca preservar os direitos de privacidade e proteção de dados dos cidadãos brasileiros.

Já o Artigo 35 regula a criação e a supervisão de cláusulas contratuais e normas corporativas que asseguram a conformidade com a LGPD durante a

IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V - quando a autoridade nacional autorizar a transferência;

VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;

VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou

IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

³²⁹ Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:

I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;

II - a natureza dos dados;

III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;

IV - a adoção de medidas de segurança previstas em regulamento;

V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e

VI - outras circunstâncias específicas relativas à transferência.

transferência internacional de dados³³⁰. Esse artigo delega à ANPD o poder de definir os conteúdos das cláusulas contratuais, que funcionam como compromissos legais para que os responsáveis pelo tratamento de dados fora do Brasil respeitem os mesmos princípios e direitos previstos pela LGPD. A ANPD também pode designar organismos de certificação para verificar a conformidade, reforçando a fiscalização e garantindo que as garantias oferecidas sejam observadas em práticas reais.

O Artigo 36 complementa o sistema ao exigir que mudanças nas garantias previamente aprovadas sejam comunicadas à ANPD³³¹. Essa obrigação de transparência permite uma revisão contínua das salvaguardas implementadas, garantindo que as práticas de proteção de dados mantenham-se alinhadas aos requisitos da LGPD. Assim, o arcabouço brasileiro para transferência internacional de dados pessoais visa a assegurar uma proteção contínua e adequada, semelhante à normativa europeia, mas adaptada ao contexto jurídico e institucional do Brasil.

Nesse campo relacionado à transferência internacional de dados pessoais, a Lei Geral de Proteção de Dados outorga também à ANPD a competência para editar regulamentos e procedimentos relativos à proteção de dados pessoais, conforme o artigo 55-J, XIII, da LGPD³³². Dentro dessa atribuição, a ANPD submeteu à Consulta

³³⁰ Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.

§ 1º Para a verificação do disposto no caput deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei.

§ 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.

§ 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.

§ 4º Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados.

§ 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei.

³³¹ Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional.

³³² Art. 55-J. Compete à ANPD: (...)

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; (Incluído pela Lei nº 13.853, de 2019).

Pública uma proposta de Regulamento de Transferências Internacionais de Dados Pessoais, visando regulamentar tais transferências e apresentar modelos de cláusulas contratuais padrão³³³.

Essa minuta abordou diversas questões essenciais, como definições, requisitos gerais, modalidades e procedimentos de aprovação para as transferências internacionais. O tema foi incluído no item 4 da Agenda Regulatória da ANPD para o biênio 2023/2024, conforme aprovado pela Portaria ANPD nº 35, de 4 de novembro de 2022. Ademais, de acordo com o artigo 5º, XV, da LGPD, a transferência internacional de dados ocorre quando dados pessoais são enviados para um país estrangeiro ou organismo internacional, e somente o compartilhamento de dados identificáveis entre agentes em países diferentes para finalidades específicas configura tal transferência, casos em que devem cumprir os requisitos legais ou regulatórios pertinentes.

Referida minuta, aprovada pelo Conselho Diretor da Autoridade Nacional de Proteção de Dados (ANPD), no mês de agosto de 2024, deu azo ao Regulamento de Transferência Internacional de Dados, registrado na forma de Resolução – Resolução CD/ANPD nº 19/2024³³⁴. Seu objetivo, portanto, é o de disciplinar o contido no capítulo V da LGPD, acerca da transferência internacional de dados pessoais – compreendendo, em referido capítulo, consoante sobredito, a redação do art. 33 ao art. 36.

Com base nos artigos 10 a 13 do Capítulo IV da Resolução CD/ANPD nº 19/2024, a decisão de adequação brasileira visa estabelecer, portanto, critérios e procedimentos para a ANPD avaliar e reconhecer a equivalência do nível de proteção de dados pessoais em países estrangeiros ou organismos internacionais, garantindo que estejam em conformidade com a LGPD e as regulamentações nacionais. A decisão de adequação funciona como um mecanismo que permite o livre fluxo de

³³³ Nesse sentido a consulta pública outrora ativa, hospedada no seguinte *link*: <https://www.gov.br/participamaisbrasil/regulamento-de-transferencias-internacionais-de-dados-pessoais-e-do-modelo-de-clausulas-padrao-contratuais#:~:text=A%20ANPD%20poder%C3%A1%20reconhecer%2C%20mediante,na%20LGPD%20e%20neste%20Regulamento>. Acesso em: 19 jul. 2024.

³³⁴Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396>. Acesso em: 09 set. 2024.

dados entre o Brasil e essas jurisdições, desde que se verifique um nível de proteção considerado compatível com as exigências brasileiras.

O Artigo 10 da Resolução CD/ANPD nº 19/2024 estabelece que a Autoridade Nacional de Proteção de Dados pode, por meio de uma decisão de adequação, reconhecer a equivalência do nível de proteção de dados de um país estrangeiro ou organismo internacional com o padrão da legislação brasileira, em especial com as diretrizes da Lei Geral de Proteção de Dados³³⁵. Esse dispositivo legitima a ANPD a avaliar e conferir a países terceiros um status de adequação, permitindo que dados pessoais sejam transferidos do Brasil para esses destinos sem a necessidade de garantias adicionais

O artigo 11 apresenta os critérios fundamentais para essa avaliação, destacando que a ANPD deve considerar não apenas a legislação vigente no país ou organização, mas também aspectos como a natureza dos dados, os princípios gerais de proteção de dados, a segurança implementada para resguardar os direitos dos titulares, e a existência de garantias institucionais independentes que assegurem a proteção efetiva dos dados pessoais³³⁶.

³³⁵ Art. 10. A ANPD poderá reconhecer, mediante decisão de adequação, a equivalência do nível de proteção de dados pessoais de país estrangeiro ou de organismo internacional com a legislação nacional de proteção de dados pessoais, observado o disposto na Lei nº 13.709, de 14 de agosto de 2018, e neste Regulamento.

³³⁶ Art. 11. A avaliação do nível de proteção de dados pessoais de país estrangeiro ou de organismo internacional levará em consideração:

I - as normas gerais e setoriais em vigor com impactos sobre a proteção de dados pessoais no país de destino ou no organismo internacional;

II - a natureza dos dados;

III - a observância dos princípios gerais de proteção de dados pessoais e dos direitos dos titulares previstos na Lei nº 13.709, de 14 de agosto de 2018;

IV - a adoção de medidas de segurança adequadas para minimizar impactos às liberdades civis e aos direitos fundamentais dos titulares;

V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e

VI - outras circunstâncias específicas relativas à transferência.

§ 1º A avaliação das normas mencionadas no inciso I do caput deste artigo será limitada à legislação diretamente aplicável ou que gere impactos relevantes sobre o tratamento de dados pessoais e sobre os direitos dos titulares.

§ 2º Para fins do disposto nos incisos III e IV do caput deste artigo, será avaliado se a legislação local estabelece aos agentes de tratamento obrigações de implementação de medidas de segurança adequadas, considerando a natureza dos dados e os riscos envolvidos no tratamento, entre outros fatores relevantes, em conformidade com os parâmetros estabelecidos na Lei nº 13.709, de 14 de agosto de 2018.

§ 3º Para fins do disposto no inciso V do caput deste artigo, serão consideradas, entre outras garantias institucionais relevantes, a existência e o efetivo funcionamento de um órgão regulador independente, com competência para assegurar o cumprimento das normas de proteção de dados e garantir os direitos dos titulares.

No artigo 12, são detalhados os fatores adicionais para a tomada de decisão da adequação, como a análise de riscos e benefícios dessa decisão para os direitos dos titulares e os potenciais impactos nas relações diplomáticas e comerciais do Brasil³³⁷. A Resolução também destaca a importância de priorizar países ou organizações internacionais que demonstrem reciprocidade ao Brasil, incentivando um fluxo de dados mais livre e seguro, desde que as garantias de proteção sejam mútuas.

Finalmente, os artigos 13 e 14 definem o procedimento para a emissão da decisão de adequação, incluindo a possibilidade de instauração, de ofício, do processo pelo Conselho Diretor da ANPD ou por solicitação de entes públicos. Esse processo inclui a avaliação técnica e a manifestação da Procuradoria Federal Especializada antes da deliberação final, visando uma abordagem estruturada e integrada para proteger os dados pessoais de acordo com os padrões da LGPD e promover uma cooperação internacional responsável³³⁸.

Vê-se, ao analisar o contido na Resolução CD/ANPD nº 19/2024, que referida normativa estabelece um modelo de governança para a transferência internacional de

³³⁷ Art. 12. Para a avaliação do nível de proteção de dados pessoais, também serão levados em consideração:

I - os riscos e os benefícios proporcionados pela decisão de adequação, considerando, entre outros aspectos, a garantia dos princípios, dos direitos do titular e do regime de proteção de dados previstos na Lei nº 13.709, de 14 de agosto de 2018; e

II - os impactos da decisão sobre o fluxo internacional de dados, as relações diplomáticas, o comércio internacional e a cooperação internacional do Brasil com outros países e organismos internacionais.

Parágrafo único. A ANPD priorizará a avaliação do nível de proteção de dados de países estrangeiros ou organismos internacionais que garantam tratamento recíproco ao Brasil e cujo reconhecimento de adequação viabilize a ampliação do livre fluxo de transferências internacionais de dados pessoais entre os países e organismos internacionais.

³³⁸ Art. 13. O procedimento para emissão de decisão de adequação:

I - poderá ser instaurado por decisão do Conselho Diretor, de ofício ou após solicitação das pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011;

II - será instruído pela área técnica competente, nos termos do Regimento Interno da ANPD, que se manifestará sobre o mérito da decisão, indicando, se for o caso, as condicionantes a serem observadas;

III - após a manifestação da Procuradoria Federal Especializada, será objeto de deliberação final pelo Conselho Diretor, na forma do Regimento Interno da ANPD.

§ 1º Os órgãos e entidades da Administração Pública com competências afetas ao tema poderão ser cientificados da instauração do processo, sendo-lhes facultada a apresentação de manifestação, no âmbito de suas competências legais.

§ 2º A decisão de adequação será proferida por Resolução do Conselho Diretor e publicada na página da ANPD na Internet.

Art. 14. O processo instaurado no âmbito da ANPD com vistas à elaboração de documentos, fornecimento de informações e quaisquer outros atos relativos ao reconhecimento do Brasil como país adequado por outro país ou organismo internacional observarão os procedimentos descritos no art. 13 deste Regulamento.

dados pessoais no Brasil, configurando-se por meio de dois principais mecanismos: a decisão de adequação e as cláusulas contratuais. A decisão de adequação, conforme o artigo 10, permite à ANPD reconhecer o nível de proteção de dados de um país estrangeiro ou organismo internacional como equivalente ao da legislação brasileira. Esse reconhecimento baseia-se em uma avaliação criteriosa da legislação e das garantias institucionais e de segurança oferecidas pelo país ou organismo, com vistas a assegurar que os direitos dos titulares de dados sejam efetivamente preservados. A decisão, portanto, promove a proteção transfronteiriça de dados, facilitando o fluxo de dados ao isentar transferências para esses países de autorizações adicionais.

Os artigos 11 e 12 complementam a decisão de adequação ao descrever os critérios de avaliação adotados pela ANPD, que incluem a natureza dos dados, a adequação das medidas de segurança, as garantias judiciais e a capacidade institucional para proteger dados pessoais no país de destino. O impacto da decisão sobre as relações comerciais e diplomáticas do Brasil também é considerado, priorizando países que ofereçam reciprocidade ao Brasil. O procedimento de emissão da decisão de adequação (art. 13) é estruturado para permitir que a própria ANPD ou entidades públicas requisitem a análise, com a decisão final sendo publicada e disponibilizada para consulta pública, o que reforça a transparência e segurança jurídica das transferências.

Quanto às cláusulas contratuais, a resolução detalha que elas constituem um mecanismo alternativo à decisão de adequação, permitindo que controladores e operadores garantam a conformidade com a LGPD por meio de contratos específicos. Essas cláusulas, sejam padrão ou específicas, devem assegurar o cumprimento dos direitos e dos princípios de proteção de dados definidos na legislação brasileira.

4.6 Comparação LGPD vs RGPD: a “decisão de adequação”

A comparação entre os sistemas europeu e brasileiro de proteção de dados, especialmente no que tange às transferências internacionais de dados pessoais, revela tanto convergências estruturais quanto divergências estratégicas e operacionais. A União Europeia, com o RGPD, e o Brasil, por meio da LGPD e da Resolução CD/ANPD nº 19/2024, buscam estabelecer padrões de proteção de dados que garantam que os dados pessoais transferidos para fora de suas fronteiras sejam

tratados com um nível de segurança e privacidade equivalente ao exigido domesticamente.

A decisão de adequação, fundamental para ambos os sistemas, reflete uma abordagem semelhante em que tanto o RGPD (Artigo 45) quanto a LGPD (Artigo 33) exigem uma análise rigorosa do país receptor. A União Europeia delega à Comissão Europeia a competência para avaliar se um país terceiro ou organização internacional oferece um nível de proteção adequado, levando em conta fatores como respeito aos direitos humanos, Estado de Direito e a existência de uma autoridade independente de proteção de dados. De maneira análoga, a ANPD, conforme estabelecido no Artigo 10 da Resolução nº 19/2024, *pode* reconhecer a adequação de países estrangeiros, considerando legislações locais, medidas de segurança e a capacidade de instituições reguladoras no país receptor.

Além da decisão de adequação, ambos os sistemas introduzem cláusulas contratuais como alternativa, especialmente para transferências com países sem *status* de adequação. O RGPD permite que empresas e organizações usem cláusulas contratuais padrão aprovadas pela Comissão Europeia (Artigo 46) como um meio de assegurar a conformidade com as normas europeias. Similarmente, a LGPD permite o uso de cláusulas contratuais específicas, com a Resolução nº 19/2024 estabelecendo os requisitos e conteúdos mínimos para tais contratos. Ambos os sistemas utilizam as cláusulas contratuais como salvaguardas para proteger dados em contextos internacionais, proporcionando uma estrutura de direitos e obrigações que, na ausência de uma decisão de adequação, previnem o tratamento inadequado de dados pessoais.

Contudo, algumas diferenças importantes surgem na implementação e aplicação dessas normativas. No contexto europeu, o RGPD exerce uma influência extraterritorial consolidada, pois aplica-se diretamente aos dados de residentes da UE, independentemente de onde estejam sendo tratados, o que confere uma forte capacidade de monitoramento e cumprimento. No Brasil, embora a LGPD também adote uma abordagem extraterritorial ao se aplicar a operações de tratamento realizadas fora do país, sua aplicação prática e capacidade de fiscalização, especialmente no contexto de decisões de adequação, ainda se encontram em fase

de maturação, sendo a independência e estrutura da ANPD temas críticos para o reconhecimento internacional de adequação, principalmente junto à União Europeia.

Além disso, a resolução brasileira se distingue ao priorizar reciprocidade nas relações internacionais. O Artigo 12 da Resolução nº 19/2024 indica que a ANPD priorizará a análise de países que garantam tratamento recíproco ao Brasil, o que agrega um componente diplomático e comercial à decisão de adequação. Esse fator destaca uma diferença estratégica em relação ao RGPD, que, embora também valorize cooperações e acordos internacionais, não enfatiza a reciprocidade como um critério explícito de análise. Essa diferença reflete as particularidades do Brasil como um ator, em um viés “ingênuo”, *emergente*, e, em uma visão crítica, *submisso* e *subalterno*, no cenário global de proteção de dados e sua necessidade de equilibrar a integração econômica com a proteção de dados pessoais – com preferência, consoante se tem visto até o momento, à primeira.

Com efeito, o Brasil, ao priorizar reciprocidade nas relações internacionais, acaba por eleger, com primazia, os entes que também se colocaram como destinados a replicar o contido na legislação europeia. Ao invés, portanto, de desejar que seu padrão de proteção de dados se coloque como pujante e autônomo, relega às decisões de proteção um caráter subalterno, de reconhecimento, com preferência, às regulamentações já formatadas de acordo com a inspiração inicial que submete os ditames de sua própria legislação.

Em verdade, conclui-se que o Regulamento Geral de Proteção de Dados europeu não obriga a Comissão Europeia a emitir decisões de adequação para todos os países terceiros ou organizações internacionais. Em vez disso, ele faculta à Comissão a possibilidade de adotar essas decisões, caso entenda que um país ou organização assegura um nível de proteção adequado aos dados pessoais equivalente ao da União Europeia. Esse procedimento envolve uma análise minuciosa da legislação e das práticas de proteção de dados do país ou organização em questão.

Quando um país terceiro ou organização solicita uma decisão de adequação com base no RGPD, portanto, não existe uma obrigação legal da Comissão Europeia de concedê-la. A Comissão tem o direito de avaliar e, se considerar apropriado, decidir sobre a emissão de uma decisão de adequação. Essa decisão não é, assim,

automática e depende de um processo de avaliação, no qual a Comissão verifica se o país solicitante oferece um nível de proteção de dados suficiente, conforme as diretrizes do RGPD. Além disso, não há prazo determinado no RGPD para que a Comissão finalize essa avaliação ou tome uma decisão, o que permite a ela um grau considerável de discricionariedade no processo. A Comissão pode ainda consultar outras entidades e membros da União Europeia para auxiliar na decisão.

Por fim, embora a Comissão Europeia não emita decisões de adequação de ofício para todos os países, ela mantém uma avaliação contínua sobre os países que já receberam a adequação, revisando as decisões a cada quatro anos ou antes, caso surjam questões significativas que indiquem que o nível de proteção pode ter caído. Ademais, na ausência de *decisão de adequação*, ela exige o cumprimento de garantias adicionais para que transferências de dados possam ocorrer de maneira segura com países não adequados, por meio de: cláusulas contratuais padrão; ou regras corporativas vinculantes para empresas multinacionais; ou derrogações específicas para situações como as de interesse público. Desse modo, o processo de adequação se apresenta como um dos diversos mecanismos para garantir essa proteção e, ao mesmo tempo, mantém outras salvaguardas em vigor para proteger os dados que saem da União Europeia³³⁹.

Na visão eurocentrada, portanto, a Comissão Europeia, ao estabelecer decisões de adequação ou promover outros instrumentos de proteção, não apenas protege os dados dos cidadãos europeus, mas também cria um *padrão global* que influencia outros países e organizações a elevarem suas práticas de proteção de dados³⁴⁰. Essa abordagem confere um poder regulatório à UE e estimula a harmonização das normas de proteção de dados em escala global, incentivando a implementação de legislações semelhantes ao RGPD em países terceiros.

³³⁹ Nesse sentido, a própria Comissão Europeia apresenta um exemplo que envolve o Brasil, demonstrando como atuam as decisões de adequação, e, na sua ausência, as normas suplementares: “Uma empresa francesa tenciona expandir os seus serviços à América do Sul, nomeadamente à Argentina, ao Uruguai e ao Brasil. O primeiro passo seria o de verificar se tais países terceiros são objeto de uma decisão de adequação. Neste caso, tanto a Argentina como o Uruguai foram declarados adequados. A empresa poderia transferir dados pessoais para estes dois países não pertencentes à UE sem garantias adicionais, ao passo que as transferências para o Brasil, que não é objeto de uma decisão de adequação, terão de ser efetuadas mediante a apresentação de garantias adequadas”. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_pt. Acesso em: 15 set. 2024.

³⁴⁰ *Idem*.

No Brasil, a questão da faculdade na emissão de *decisões de adequação* não guarda conclusão distinta da europeia, já que é igualmente marcada pela ausência de obrigatoriedade, mas com nuances que refletem a particularidade de sua posição regulatória “emergente”. Conforme disposto no Artigo 10 da Resolução CD/ANPD nº 19/2024, a ANPD possui a competência para emitir decisões de adequação, mas tal poder é discricionário e não implica uma obrigatoriedade de reconhecer qualquer país ou organização como adequado. Essa similaridade com a União Europeia revela que o Brasil adota, ao menos em princípio, uma postura na qual a ANPD mantém o direito de realizar uma análise minuciosa e independente antes de conceder a adequação, sem a exigência de atender a todas as solicitações recebidas.

Contudo, ao contrário da União Europeia, onde a Comissão Europeia exerce uma autoridade consolidada e reconhecida na emissão e revisão dessas decisões, a ANPD ainda busca firmar-se como uma autoridade reguladora com autonomia plena e capacidade de influenciar o cenário internacional de proteção de dados. A ausência de decisões de adequação no Brasil até o momento, especialmente em relação à União Europeia, reflete essa dificuldade em obter um reconhecimento global robusto e revela a existência de desafios institucionais e diplomáticos que precisam ser superados para que o Brasil possa atuar com maior protagonismo regulatório.

Adicionalmente, embora a ANPD, assim como a Comissão Europeia, possa escolher outras garantias de proteção de dados para compensar a ausência de decisões de adequação — como cláusulas contratuais específicas ou normas corporativas globais —, a capacidade de fiscalização e a estrutura da ANPD são incipientes frente à realidade do trânsito internacional de dados pessoais, e, portanto, temas que necessitam de intenso debate e desenvolvimento. Enquanto a União Europeia já consolidou suas cláusulas contratuais padrão como salvaguardas amplamente aceitas e eficazes, o Brasil, na condição de nação periférica, se encontra em um estágio diferente de maturidade entre as regulamentações, onde o RGPD atua como uma referência consolidada e a LGPD se encontra em uma fase de adaptação e expansão de sua aplicabilidade prática.

Ante o exposto, tanto na União Europeia quanto no Brasil, a emissão de decisões de adequação permanece uma faculdade discricionária das autoridades de proteção de dados, e não uma obrigação. Todavia, as consequências desse caráter

facultativo refletem-se de forma distinta: enquanto a União Europeia utiliza esse poder para influenciar práticas globais, o Brasil busca uma adequação que o permita estabelecer relações comerciais e políticas mais integradas e harmônicas com os padrões europeus, evidenciando uma dependência que ainda limita seu potencial regulatório autônomo.

4.7 O dever de uma “decisão de adequação” brasileira como resposta democrática ao poder da privacidade, ao neoliberalismo e ao colonialismo de dados

O conceito de democracia, especialmente em sua expressão moderna, implica não apenas um regime onde os cidadãos participam ativamente na definição das direções políticas de sua sociedade, mas também um compromisso com a proteção dos direitos fundamentais, entre os quais se encontra, de forma crescente, o direito à proteção de dados pessoais. Desde a promulgação da Constituição Federal de 1988, o Brasil se consolidou como um Estado Democrático de Direito, onde a dignidade humana e os direitos dos cidadãos são pilares centrais. Esse compromisso democrático encontra no direito à privacidade, intimamente relacionado à proteção de dados pessoais, um novo campo de atuação essencial para o exercício das liberdades individuais em uma era marcada pela transformação digital.

A proteção dos dados pessoais em democracias contemporâneas é crucial para a manutenção do espaço público democrático, no qual as liberdades individuais e coletivas possam ser exercidas sem interferência desproporcional de agentes privados ou governamentais. A transformação da informação em um recurso econômico e político poderoso impõe a necessidade de limites claros à exploração desses dados, especialmente nas transferências internacionais. Quando dados pessoais são compartilhados com países em que a proteção de dados é menos rigorosa ou sequer existe, por um lado, ou mesmo com países de proteção dita robusta e suficiente, mas que se beneficiam de seu poder como Estados centrais para explorar nações periféricas, cidadãos de países como o Brasil tornam-se vulneráveis ao que se denomina “colonialismo de dados” — uma prática onde dados oriundos de países com proteção limitada ou menos desenvolvida acabam sendo utilizados de maneira exploratória por grandes corporações e, em alguns casos, por Estados estrangeiros.

Esse processo cria uma nova forma de desigualdade e ameaça a autonomia dos indivíduos e a soberania informacional do Estado.

A democracia é, antes de tudo, um compromisso profundo com a proteção da dignidade humana e com o respeito aos direitos fundamentais que asseguram a liberdade e a igualdade dos cidadãos em um espaço público participativo. Ela não se limita a um sistema de eleições periódicas, mas se manifesta, em sua essência, como uma estrutura de governança que coloca o indivíduo no centro das decisões que impactam a sociedade, desde os aspectos políticos e econômicos até os informacionais. Em tempos de transformação digital, a democracia moderna precisa, mais do que nunca, defender os direitos dos cidadãos frente ao poder de entidades privadas e estatais, que, pela exploração e controle das informações pessoais, podem influenciar, moldar e até limitar a autonomia individual. Desse modo, a verdadeira democracia é aquela que garante um ambiente seguro, onde cada cidadão possa se desenvolver e participar plenamente, com o amparo de instituições que protejam seus direitos, inclusive no domínio digital. É por isso que a soberania informacional se torna uma extensão indispensável do próprio exercício democrático, assegurando que o controle sobre os dados permaneça nas mãos dos indivíduos e que o Estado se posicione como defensor desses interesses frente às pressões globais, e mesmo das elites nacionais.

A análise da proteção de dados como princípio constitucional democrático revela, portanto, um compromisso profundo com a salvaguarda da dignidade humana e a preservação de um espaço público democrático. Como destacado por Danilo Doneda, esse direito transcende a mera proteção à privacidade individual, conectando-se diretamente à manutenção de liberdades fundamentais, como a liberdade de expressão, a participação política e o livre desenvolvimento da personalidade. Ao inserir a proteção de dados como um direito fundamental na Constituição Federal, a Emenda Constitucional nº 115/2022 fortalece o arcabouço jurídico necessário para garantir que os cidadãos tenham controle sobre suas informações em um cenário globalizado, onde o fluxo de dados pessoais desafia as fronteiras nacionais e expõe os indivíduos a riscos de controle e manipulação por atores privados e estatais.

Nesse sentido, a positivação desse direito reforça a necessidade de um Estado atento às mudanças tecnológicas, que afetam tanto a estrutura social quanto os direitos dos cidadãos. A proteção de dados pessoais se posiciona, assim, como um pilar essencial de uma democracia que valoriza a transparência, a responsabilização e o respeito à autonomia individual. Ao estabelecer padrões para a coleta e uso de dados, a Constituição brasileira e a LGPD devem convergir para assegurar que a prática democrática não seja comprometida por práticas de vigilância indiscriminada, evitando que a manipulação de informações pessoais resulte em discriminação, exploração ou exclusão – situações, no mais das vezes, ínsitas à própria economia baseada em dados pessoais.

Danilo Doneda, ao longo de sua obra, argumenta que a proteção de dados pessoais representa uma fronteira fundamental de resistência contra o abuso de poder, seja ele estatal ou privado. Essa proteção é particularmente relevante em um contexto, consoante sobredito, de "colonialismo de dados", em que grandes corporações multinacionais, detentoras de tecnologias avançadas de coleta e análise de dados, obtêm informações pessoais de cidadãos de países com regulações menos desenvolvidas, ou de capacidade de resistência diminuída diante de sua dependência econômica e tecnológica, em uma lógica de submissão que ultrapassa o fenômeno do próprio "colonialismo de dados" em prol de um verdadeiro "neocolonialismo", em que a faceta dos dados é o aspecto mais visível e poderoso dessa engrenagem. Esse fenômeno, que fere princípios democráticos ao deslocar o poder informacional dos indivíduos para entidades que não estão submetidas ao controle democrático, exige uma resposta robusta por parte do Estado, que, ao adotar normas como a *decisão de adequação*, deve visar a garantia de que transferência internacional de dados ocorra sob um regime de proteção rigoroso e compatível com a dignidade humana e a vida real dos brasileiros e brasileiras, com suas vidas "vivíveis"³⁴¹ em contexto latino-americano e periférico.

Por fim, ao analisar a Emenda Constitucional nº 115/2022, Ingo Wolfgang Sarlet destaca que o reconhecimento constitucional da proteção de dados pessoais

³⁴¹ Expressão empregada por Judith Butler, ao defender o Poder constituinte como um agenciamento multiforme de precariedades que reivindicam vidas mais "vivíveis" comprometidas radicalmente com a democracia igualitária. (BUTLER, 2019, p. 28).

no Brasil representa um marco na defesa dos direitos fundamentais. Esse avanço coloca o Brasil em consonância com as tendências globais de constitucionalização do direito à privacidade e à proteção de dados, conferindo a esse direito um status jurídico de primeira ordem, com aplicabilidade imediata e vinculativa. O constitucionalista observa que, embora a LGPD tenha sido um grande avanço no campo da proteção de dados, sua consolidação no texto constitucional fornece uma base mais sólida e permanente para a tutela desse direito. Ressalta, ainda, que a inclusão do direito à proteção de dados no rol de direitos fundamentais implica que as normas infraconstitucionais devem respeitar os limites impostos pela Constituição, impedindo a criação de legislações que possam enfraquecer a proteção dos dados pessoais dos cidadãos – o que deve impactar, sobremaneira, a própria leitura, interpretação e confecção de normas destinadas, *v.g.* a regular a transferência internacional de dados pessoais.

Dessa forma, o direito à proteção de dados pessoais se consolida como um princípio essencial para o fortalecimento da democracia no Brasil, promovendo a inclusão social e garantindo que todos os cidadãos, especialmente os mais vulneráveis, possam participar de uma sociedade que respeite sua privacidade e autodeterminação informativa. A Constituição e a LGPD, ao estabelecerem diretrizes para a coleta e uso de dados, devem obrigatoriamente assegurar um ambiente em que o poder democrático permaneça nas mãos dos cidadãos, protegendo-os contra abusos informacionais e promovendo um modelo de governança onde a dignidade humana e a justiça social sejam princípios norteadores.

Reconhecer o que se afirma significa ir ao encontro da perspectiva da tropicalização do pensamento sobre proteção de dados pessoais no Brasil, a partir do que o conceito de soberania informacional ganha contornos específicos que vão além da simples adaptação de normas estrangeiras, como o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia. A soberania informacional envolve a capacidade de um Estado, no caso brasileiro, de proteger e regular os fluxos de dados pessoais de seus cidadãos de modo autônomo e condizente com as necessidades e vulnerabilidades locais. Em uma posição periférica no cenário global, o Brasil precisa considerar como as práticas de coleta e tratamento de dados refletem interesses que nem sempre estão alinhados com a proteção dos direitos fundamentais da sua

população. A ideia de soberania informacional busca justamente estabelecer uma governança de dados que reforce a autonomia nacional e assegure que os dados pessoais dos cidadãos brasileiros não sejam explorados ou manipulados para fins que contrariem o interesse público, no sentido mais profundo de interesse do *povo brasileiro* – respeitadas as nuances mais profundas de compreensão desse termo, que deve ser reconhecido, nos dizeres de Friedrich Müller, como *destinatário das prestações civilizatórias do Estado*, e que vive, ainda hoje, o drama de se reconhecer na ambivalência apresentada por Darcy Ribeiro, ao mesmo tempo como *povo novo* e como *povo velho*.

A Agência Nacional de Proteção de Dados (ANPD) emerge nesse cenário como o órgão regulador central, responsável por zelar pela integridade dos dados pessoais dos cidadãos e assegurar que a transferência internacional de dados ocorra dentro de um marco regulatório robusto. A ANPD, ao exercer suas funções de fiscalização e controle, enfrenta o desafio de estabelecer uma postura firme e independente diante de gigantes tecnológicos globais e de interesses estrangeiros que utilizam dados como recursos econômicos. A emissão de decisões de adequação pela ANPD, como instrumento de verificação da compatibilidade entre os níveis de proteção do Brasil e de países terceiros, torna-se essencial para a soberania informacional, pois permite que o Brasil condicione a transferência de dados à existência de garantias que respeitem os padrões estabelecidos pela LGPD.

Esse ponto é de importância fundamental e merece ecoar com intensidade proporcional a tudo que se vêm afirmando: a decisão de adequação figura como um instrumento poderoso, indispensável para a afirmação de uma soberania informacional brasileira que não se limite a repetir normas estrangeiras, mas que responda às necessidades do país e de seu povo em um contexto de constante transformação digital. Ela é essencial não apenas para garantir que dados pessoais sejam tratados de acordo com a dignidade humana, mas também para assegurar que o Brasil possua controle sobre o destino e o uso desses dados, limitando interferências de interesses externos que busquem explorar as informações dos cidadãos para fins comerciais, políticos ou de vigilância. Para que isso se efetive, a ANPD deve operar de forma independente e robusta, pautando-se por critérios rigorosos que privilegiem a proteção dos direitos fundamentais sobre pressões econômicas e comerciais,

adotando, para tanto, uma postura proativa, diferentemente da visão facultativa de adequação adotada pela atual redação da Resolução em vigor, em um verdadeiro exercício de autodeterminação e resistência, em que o direito à proteção de dados pessoais se apresenta como um elemento central de uma democracia verdadeira, factível, real, moderna e inclusiva.

Em vez de ver a decisão de adequação como uma opção, a ANPD precisa integrá-la como um elemento estrutural de sua função regulatória, assegurando que os países destinatários dos dados brasileiros cumpram requisitos de segurança, transparência e proteção contra abusos. Isso implica que a agência deve desenvolver e aplicar um conjunto de critérios rigorosos ao avaliar se um país oferece proteção equivalente àquela conferida pela LGPD, abordando, entre outros fatores, o respeito à dignidade humana, a transparência no tratamento de dados e o direito dos cidadãos à autodeterminação informativa – em detrimento, se necessário, dos ganhos financeiros advindos da inerente transferência de dados pessoais em diferentes atividades econômicas.

Não se quer, com referido posicionamento, isolar o país do contexto internacional. Ao revés. A soberania informacional brasileira, nesse sentido, requer uma atuação assertiva e diplomática da ANPD, que deve estabelecer parcerias e diálogos internacionais, mas sem abrir mão dos princípios fundamentais de proteção, que devem figurar com pontos fixos, impassíveis de negociação em troca de ganhos financeiros particulares, em detrimento de potenciais ataques a direitos individuais e coletivos advindos da proteção constitucional aos dados pessoais. A "tropicalização" dessa soberania informacional inclui, portanto, a consideração dos contextos socioeconômicos e tecnológicos locais, onde as disparidades de acesso à tecnologia e a falta de conhecimento sobre proteção de dados são realidades marcantes. A ANPD deve, portanto, promover a educação e conscientização sobre o direito à privacidade e à proteção de dados, garantindo que cidadãos de todas as esferas sociais compreendam seus direitos e possam exercê-los plenamente, inclusive no contexto de transferência internacional de dados.

Ademais, a ANPD deve estar preparada para enfrentar pressões econômicas e políticas que possam surgir em negociações internacionais. A tropicalização do pensamento sobre proteção de dados não significa apenas a adoção de normas

globais, mas a adaptação crítica dessas normas para que respondam às particularidades e necessidades brasileiras. Assim, ao construir uma política de soberania informacional, a ANPD não pode limitar-se a replicar modelos europeus; ao contrário, deve desenvolver uma abordagem que fortaleça o protagonismo do Brasil na defesa dos direitos digitais de seus cidadãos, assegurando que qualquer transferência internacional de dados ocorra sob condições que respeitem e preservem a autonomia e dignidade do indivíduo no ambiente digital. E a intransigência internacional de países dito centrais deve ser respondida com coragem e altivez, representadas pela firme posição nacional em não recuar um único passo na proteção de dados pessoais de seus cidadãos, ciente do contexto predatório em que tais dados habitam.

Essa abordagem tropicalizada da ANPD envolve, portanto, um compromisso contínuo com a criação e manutenção de normas de proteção que considerem tanto as práticas e padrões globais quanto às peculiaridades da sociedade brasileira. A soberania informacional, ao ser orientada por esse modelo de tropicalização, não só resguarda os dados dos cidadãos brasileiros de possíveis abusos e vigilâncias externas, mas também contribui para a consolidação de um Estado que valoriza a proteção da privacidade como um pilar de sua democracia.

A construção de um conceito de soberania informacional no Brasil se entrelaça, portanto, com um exercício de tradução e interpretação jurídica, especialmente no que diz respeito à proteção de dados pessoais em um contexto de forte influência internacional, onde o direito comparado e os estudos mais profundos acerca das “tradições” jurídicas devem desempenhar um papel fundamental. A legislação brasileira sobre proteção de dados, expressa na LGPD, ainda que inspirada pelo Regulamento Geral de Proteção de Dados da União Europeia, precisa assumir, cada vez mais, características próprias ao ser adaptada à realidade nacional. Nesse sentido, o que se poderia interpretar como um mero transplante jurídico do RGPD para o Brasil precisa se revelar, na prática, como uma tentativa permanente de tradução que exige uma contínua adaptação e interpretação por parte dos operadores do direito brasileiros.

A Agência Nacional de Proteção de Dados (ANPD) ocupa, conforme afirmado, posição central neste processo de construção da soberania informacional, sendo

responsável por estabelecer critérios de compatibilidade com os padrões de proteção de dados de outros países, especialmente em relação às transferências internacionais de dados pessoais. A soberania informacional aqui assume uma dimensão crítica ao se traduzir em práticas regulatórias que buscam resguardar os interesses e direitos dos cidadãos brasileiros em um contexto global, onde esses dados se tornaram insumos valiosos para as economias mais avançadas. A ANPD, ao decidir sobre a adequação dos regimes de proteção de dados de outros países, não apenas promove a integração do Brasil com normas globais, mas também afirma a autonomia nacional, determinando salvaguardas específicas para a proteção de dados de brasileiros no exterior.

Contudo, a abordagem adotada pela ANPD, que faculta a avaliação dos países destinatários em vez de obrigá-la, traz à tona questionamentos sobre o real alcance dessa soberania informacional. A ausência de uma obrigatoriedade formal para a análise de adequação compromete, em certa medida, a eficácia da proteção dos dados pessoais dos brasileiros, especialmente quando essas informações são transferidas para jurisdições que não oferecem as mesmas garantias. Esse modelo regulatório deixa à ANPD uma margem de discricionariedade que pode gerar insegurança quanto à proteção de dados transnacional, além de revelar uma possível fragilidade no compromisso com a efetiva soberania informacional do país, especialmente diante das pressões econômicas e políticas globais.

Além da decisão de adequação, a Resolução CD/ANPD nº 19/2024 e a própria LGPD introduzem as cláusulas contratuais padrão como um dos principais instrumentos para viabilizar a transferência internacional de dados pessoais. Esse mecanismo, embora útil em contextos de maior equilíbrio de poder entre as partes, demonstra-se problemático em um cenário como o brasileiro, onde o país ocupa uma posição fraca nas negociações globais e onde empresas e Estados estrangeiros, muitas vezes com interesses conflitantes com os valores e necessidades locais, são os principais destinatários desses dados. Deixar a garantia de proteção de dados ao âmbito contratual, entre agentes privados e em uma situação de evidente disparidade de poder, é uma solução que não condiz com os princípios democráticos que deveriam pautar a proteção dos direitos fundamentais dos cidadãos brasileiros. A responsabilidade pela proteção da privacidade e da soberania informacional não pode

ser terceirizada a acordos comerciais que, no mais das vezes, refletem a lógica de mercado, e não a de preservação dos direitos e da dignidade humana.

A dependência das cláusulas contratuais padrão para assegurar a proteção de dados representa, assim, uma concessão às dinâmicas neoliberais, onde o livre fluxo de capital e dados prevalece sobre o respeito aos direitos fundamentais. Esse modelo de proteção flexibilizada ignora o contexto de vulnerabilidade regulatória e econômica que países como o Brasil enfrentam, uma vez que cláusulas contratuais muitas vezes são impostas unilateralmente por empresas multinacionais, deixando ao Brasil pouca margem para definir suas próprias exigências em matéria de proteção de dados. Em uma verdadeira democracia, é o Estado, e não o mercado, quem deve assegurar o cumprimento de normas que garantam a inviolabilidade da privacidade e da dignidade dos cidadãos. O fato de a ANPD confiar em mecanismos privados para regular a transferência de dados revela um descompasso entre os objetivos democráticos da legislação e a realidade prática de sua aplicação, colocando em risco a efetividade dos direitos de proteção de dados.

Dessa forma, ao permitir que as cláusulas contratuais padrão assumam um papel central na proteção dos dados dos cidadãos, a ANPD falha em seu papel de guardião dos direitos fundamentais, deixando a população brasileira vulnerável à exploração informacional. Esse instrumento não oferece garantias suficientes em um contexto de assimetria de poder e falha em atender às exigências de um Estado Democrático de Direito, que deveria agir proativamente na defesa de seus cidadãos. Ao negligenciar a necessidade de regulamentações mais rígidas e de um controle estatal efetivo, a ANPD subordina o direito à privacidade a interesses comerciais, desconsiderando que a proteção de dados é um direito fundamental que deve ser defendido de maneira intransigente, sobretudo em negociações com parceiros que detêm maior poder econômico e político.

É aqui que a tropicalização do pensamento jurídico, aliada ao conceito de tradução jurídica, torna-se essencial para a ANPD. A autoridade deve exercer seu papel interpretativo não apenas com o intuito de reproduzir as normas e práticas europeias, mas também de reformulá-las à luz das necessidades brasileiras. Esse processo exige um compromisso mais firme com uma interpretação que privilegie a proteção dos cidadãos nacionais e resista ao simples alinhamento com interesses

comerciais de potências econômicas. A ANPD deve, assim, adotar um posicionamento que reafirme a soberania informacional brasileira, ainda que inspirada no RGPD, impondo critérios de adequação que atendam aos interesses brasileiros e não apenas aos padrões europeus.

Para que a ANPD exerça um papel verdadeiramente soberano e representativo dos interesses nacionais, a tropicalização do pensamento jurídico precisa envolver um processo de adaptação não apenas formal, mas substantivo. Isso inclui desenvolver uma metodologia de análise de adequação que leve em conta as vulnerabilidades específicas do Brasil, como a falta de acesso amplo à educação sobre proteção de dados, a vulnerabilidade a invasões cibernéticas e a exploração econômica de dados por parte de grandes corporações alienígenas e de Estados estrangeiros. Essa postura intransigente na avaliação das condições de proteção oferecidas pelos países destinatários dos dados brasileiros reflete não apenas um compromisso com a proteção de dados em si, mas com a autonomia nacional, garantindo que os direitos e as expectativas dos cidadãos brasileiros sejam plenamente resguardados.

A ANPD precisa operar, portanto, com um rigor adequado para enfrentar o fenômeno do “colonialismo de dados”, em que o controle dos fluxos de dados por empresas e nações mais desenvolvidas no mais das vezes impõe um modelo extraterritorial, influenciando a forma como países em desenvolvimento gerenciam seus recursos informacionais. A adoção de decisões de adequação pela ANPD deve se afastar de um mero alinhamento formal ao RGPD, construindo uma abordagem que considere as vulnerabilidades e os interesses do Brasil, posicionando o país como ator capaz de proteger sua população dos efeitos prejudiciais da exploração de dados.

Ao avaliar regimes estrangeiros para permitir a transferência internacional de dados, a ANPD, deve estabelecer requisitos claros e intransigentes, assegurando que apenas países com padrões compatíveis aos da LGPD e de outras normas voltadas à proteção dos dados pessoais dos cidadãos nacionais possam ter acesso aos dados pessoais dos brasileiros. Esse processo vai além da proteção individual; ele reforça, diga-se novamente, a soberania brasileira, impedindo que informações sensíveis da população sejam usadas para fins que possam, em última instância, comprometer a democracia e a privacidade dos cidadãos.

Além disso, a ANPD deve lidar com as pressões do neoliberalismo, que muitas vezes privilegia a liberdade de mercado e o livre fluxo de informações em detrimento da proteção individual. Essas influências neoliberais pressionam países a abrir seus mercados de dados, muitas vezes em termos que favorecem corporações transnacionais. No entanto, ao interpretar e aplicar a LGPD, a ANPD pode — e deve — adotar uma postura que priorize a vida real e os direitos dos brasileiros. Isso significa que, ao aprovar a transferência de dados, a ANPD deve exigir salvaguardas suficientes que evitem que os dados pessoais sejam explorados de forma a exacerbar as desigualdades sociais e econômicas já existentes no Brasil.

Esse cenário é emblemático da maneira como o neoliberalismo molda políticas públicas e legislações de proteção de dados no Sul global. A LGPD, ao estabelecer um regime de proteção de dados em consonância com as demandas globais, tenta posicionar o Brasil como um país comprometido com a privacidade e a segurança dos cidadãos. No entanto, as pressões do mercado global — oriundas especialmente de corporações do Norte global — tensionam esse regime e acabam impondo exigências que enfraquecem a autonomia regulatória nacional. A ausência de um compromisso explícito com a obrigatoriedade das decisões de adequação exemplifica essa dicotomia, pois a flexibilidade oferecida à ANPD pode levar a concessões que limitam a proteção dos dados pessoais em favor de interesses comerciais.

Diante disso, a construção jurídica da soberania informacional no Brasil requer não apenas uma legislação robusta, mas uma postura ativa do Estado na defesa dos direitos de privacidade e proteção de dados. A ANPD, como órgão regulador, desempenha um papel fundamental nesse processo, mas enfrenta desafios relacionados à dependência financeira e às limitações estruturais, que podem comprometer sua autonomia frente a pressões econômicas. Para que a soberania informacional seja efetiva, é necessário que a ANPD não apenas tenha capacidade normativa e fiscalizadora, mas também independência política e recursos que assegurem sua operação livre de influências externas.

Assim, o fortalecimento da LGPD e da ANPD passa pela consolidação de uma política nacional de proteção de dados que seja imune às flutuações do mercado internacional e que garanta uma verdadeira independência regulatória. Isso implica

em resistir às dinâmicas do colonialismo de dados, que, ao se manifestarem no campo digital, reforçam a subordinação econômica e cultural do Sul global. A proteção dos dados brasileiros, ao transcender uma função puramente técnica, se torna um ato de resistência contra as forças que visam transformar a privacidade em mercadoria, reafirmando a autonomia do país em um cenário global onde a hegemonia neoliberal tende a enfraquecer os direitos e a soberania dos Estados periféricos.

A construção de uma soberania informacional envolve também o fortalecimento da educação sobre a importância da privacidade e da proteção de dados. A conscientização pública sobre os direitos relacionados aos dados pessoais, além de facilitar o cumprimento da LGPD, empodera a população para que esta participe ativamente da defesa de seus próprios interesses informacionais. Para que a proteção de dados seja efetiva e compreendida como um direito fundamental, é crucial que o Estado, em conjunto com a sociedade civil, invista em políticas educacionais e campanhas de conscientização que reforcem a importância de uma cidadania digital ativa e informada.

Com isso, a proteção dos dados pessoais deixa de ser um imperativo meramente técnico ou burocrático e se transforma em um projeto de autonomia nacional, essencial para a proteção da democracia e para a construção de uma sociedade *informacionalmente* soberana.

Em linha com as perspectivas teóricas discutidas, o conceito e a prática efetiva de uma postura condizente com uma soberania informacional surgem no Brasil como resposta jurídica e política ao “colonialismo de dados”, ao neoliberalismo e ao poder advindo da privacidade e da capacidade e dos interesses de subjuga-la por meio da predação e tratamento de dados pessoais, buscando assegurar que a gestão e o tratamento dos dados respeitem a autonomia nacional e a dignidade dos cidadãos. A soberania informacional visa a estabelecer o direito do país em controlar o uso e a destinação dos dados de seus cidadãos, protegendo-os das dinâmicas de poder das grandes plataformas digitais que operam com pouca ou nenhuma supervisão local. A Lei Geral de Proteção de Dados, ao regular as condições de tratamento e transferência de dados, posiciona-se como um marco inicial nesse processo de proteção jurídica, embora os desafios ainda persistam, conforme resta claro na redação deste trabalho, na implementação e supervisão das suas normas.

A ANPD, enquanto órgão regulador da LGPD, assume um papel essencial para garantir que a soberania informacional brasileira não seja uma promessa vazia. No entanto, a efetividade da ANPD depende de sua capacidade de monitoramento e aplicação das normas de forma independente e rigorosa, especialmente no cenário há pouco desenhado, em que as grandes corporações globais detêm vasto poder econômico e político. A ANPD, embora criada para assegurar o cumprimento da LGPD, ainda enfrenta limitações próprias da postura nacional submissa aos ditames internacionais, o que impacta diretamente sua capacidade de fiscalização e aplicação das diretrizes legais, especialmente em casos de transferência internacional de dados. Dessa forma, o potencial da ANPD para operar como um verdadeiro guardião da soberania informacional está vinculado à sua autonomia e capacidade de enfrentamento das pressões das corporações que dominam o mercado de dados globalmente, bem como o interesse de Estados estrangeiros e de uma elite nacional capaz de se beneficiar, política e economicamente, de um panorama inadequado de prestígio ao direito constitucional à proteção de dados dos nacionais brasileiros.

A prática de colonialismo de dados no Brasil, conforme elucidado por autores como Nick Couldry, Ulises A. Mejias e teóricos brasileiros, acentua a necessidade de proteção das informações pessoais, que são sistematicamente capturadas, processadas e monetizadas por empresas estrangeiras. Esses dados, ao serem enviados para fora do país, escapam do controle das autoridades locais, expondo os cidadãos a um risco ampliado de manipulação e exploração. É nesse ponto que a LGPD e outras iniciativas voltadas à proteção de dados pessoais, mormente na perspectiva da transferência internacional de dados pessoais, se tornam cruciais: ao estabelecerem critérios para a adequação da proteção de dados nos países destinatários, se mostram, em tese, capazes de oferecer uma ferramenta para assegurar que os dados brasileiros sejam tratados em conformidade com as normas e princípios nacionais. Essa “decisão de adequação” opera como uma medida de resistência à lógica colonial, estabelecendo barreiras contra a exploração indiscriminada dos dados e permitindo que o Brasil tenha voz ativa na proteção de seus cidadãos no cenário digital global.

Por fim, o contexto do Sul Global e, em particular, o caso brasileiro, demonstram que a luta pela soberania informacional vai além da regulação técnica;

trata-se de uma questão de autonomia e de direito à autodeterminação digital. O fortalecimento da ANPD e a aplicação rigorosa da LGPD constituem os primeiros passos para que o Brasil avance rumo à emancipação digital e ao enfrentamento das dinâmicas de poder que perpetuam o colonialismo de dados. A construção de uma infraestrutura digital própria e a promoção de tecnologias desenvolvidas localmente são medidas essenciais para garantir que a soberania informacional não seja apenas uma proteção reativa, mas também um projeto proativo de construção de um ecossistema digital alinhado com os interesses e direitos da população brasileira.

Ao adotar uma postura que privilegia a proteção da privacidade dos cidadãos em detrimento de concessões às pressões comerciais, a ANPD pode se consolidar, portanto, como um instrumento – e, quiçá, o mais importante – de construção e consolidação de uma soberania informacional. Essa construção, no entanto, demanda uma abordagem multifacetada, a exemplo da aqui realizada, que compreenda as complexidades do neoliberalismo, do poder da privacidade e do “colonialismo de dados”, em que as corporações globais do Norte frequentemente ditam os termos da circulação informacional. A política de adequação, neste caso, representa mais que uma decisão administrativa; ela simboliza um compromisso com o exercício de uma regulação informacional soberana, que se recusa a abrir mão da autonomia dos dados em benefício de forças econômicas externas.

A resistência às pressões externas e aos desejos de uma *elite exógena*, retomando Darcy Ribeiro, passa, portanto, pela definição de uma política de adequação que seja firmemente aliada da Constituição brasileira e da democracia, e, portanto, orientada pela proteção dos direitos fundamentais dos cidadãos brasileiros. Esta resistência, se levada a sério pela ANPD, implica a imposição de critérios rigorosos de proteção e segurança, exigindo que os parceiros comerciais internacionais respeitem os parâmetros de proteção de dados estabelecidos pela legislação brasileira. Isso torna a política de adequação não apenas um mecanismo de controle sobre a transferência de dados, mas um instrumento que obriga o reconhecimento e o respeito ao modelo de privacidade brasileiro, reforçando a posição do Brasil como um ator autônomo na cena digital.

Diante de tais considerações, o caminho da ANPD rumo a uma soberania informacional plena exige uma infraestrutura regulatória que vá além das simples

adaptações às práticas internacionais dominantes. Trata-se de promover uma estrutura que reflita as particularidades culturais, sociais e econômicas do Brasil, posicionando a proteção de dados como uma área estratégica para o desenvolvimento nacional, em um âmbito em que a decisão de adequação se torna uma resposta concreta aos ataques supramencionados, na medida em que promove a reciprocidade e a simetria nas relações de troca informacional entre o Brasil e outros países. Essa reciprocidade, essencial para a justiça informacional, subverte a lógica de exploração e reafirma o direito dos cidadãos brasileiros de controlar seus dados, estabelecendo um marco que se contrapõe ao fluxo unilateral e predatório característico do neoliberalismo digital.

Essas são as razões, trabalhadas e retrabalhadas, pelas quais a LGPD, apesar de sua inspiração no RGPD europeu, deve ser analisada sob uma ótica crítica que compreenda a necessidade de adequação às realidades brasileiras. A “decisão de adequação” para transferência internacional de dados, um dos pontos centrais para a construção de soberania informacional, destaca-se como essa ferramenta crucial. A interpretação crítica das normas e diretrizes internacionais, como a que influenciou a LGPD, destaca a importância de não apenas replicar o RGPD, mas de desenvolver uma legislação que reflita a realidade socioeconômica do Brasil. Este posicionamento requer que as “decisões de adequação” sejam tratadas como uma obrigação regulatória, e não apenas uma faculdade da ANPD, em que a Autoridade deve se sentir disposta e capaz de resistir às pressões do mercado e de potências estrangeiras.

O desenvolvimento de uma política nacional de proteção de dados robusta e alinhada com os interesses locais reforça a posição do Brasil como um ator ativo no cenário global de proteção de dados. Isso significa que a decisão de adequação, quando interpretada e aplicada rigorosamente, se torna um instrumento não só de proteção da privacidade, mas de um compromisso com uma soberania informacional genuína, em que o Brasil não será apenas um receptor passivo das regras impostas por potências estrangeiras, mas um país capaz de ditar seus próprios termos na economia digital.

Dessa forma, a criação de um arcabouço normativo que resista às influências neoliberais e proteja os direitos informacionais dos cidadãos brasileiros é um passo

essencial para o fortalecimento da democracia digital e da autonomia nacional. A ANPD, em sua missão regulatória, desempenha um papel central na construção dessa soberania, e a forma como ela se posiciona diante das transferências internacionais de dados será decisiva para consolidar a autonomia do Brasil na era digital.

No entanto, a verdade é que a ANPD, na esteira do que vem se revelando a atividade regulatória dos dados pessoais no Brasil, e apesar de todo o exposto, falha em cumprir seu papel fundamental de defesa intransigente da privacidade e da proteção dos dados pessoais dos cidadãos brasileiros. Aprovando a Resolução CD/ANPD nº 19/2024, a agência não apenas cede a pressões internacionais e interesses econômicos, mas também se desvia das exigências democráticas que pautam sua criação. O compromisso da ANPD deveria ser o de atuar como um bastião da soberania informacional e como guardião dos direitos fundamentais, colocando a proteção dos dados pessoais e o respeito à privacidade dos cidadãos no centro de suas decisões. No entanto, ao regulamentar a transferência internacional de dados de forma permissiva e não-impositiva, a ANPD prioriza um alinhamento com normas externas, desconsiderando as peculiaridades e vulnerabilidades da sociedade brasileira e comprometendo, assim, a autonomia regulatória que deveria defender.

Essa postura reflete uma desconexão entre as diretrizes da Constituição Federal, que preconiza a defesa da dignidade humana e da autodeterminação, e a prática regulatória adotada pela ANPD. Em vez de promover uma política de proteção de dados que reflita um compromisso com a justiça social e a democracia, a agência sucumbe à lógica neoliberal de flexibilização dos direitos fundamentais em favor do comércio global e dos interesses de corporações estrangeiras. Esse comportamento fragiliza o arcabouço democrático, pois a ANPD, ao permitir a flexibilização das transferências internacionais de dados, compromete a própria função pública que lhe foi atribuída: a de assegurar que os cidadãos brasileiros estejam protegidos contra o uso indevido e exploratório de suas informações pessoais. Ao relegar suas responsabilidades e adotar uma postura submissa, a ANPD abdica de seu papel constitucional e coloca em risco a proteção da soberania informacional brasileira.

Ademais, o processo legislativo da LGPD, apesar de representar um avanço significativo na proteção de dados pessoais no Brasil, revela uma série de limitações

e compromissos que enfraquecem sua capacidade de assegurar uma soberania informacional robusta. Desde a sua concepção, o projeto de lei esteve permeado pela necessidade de alinhar o Brasil aos padrões internacionais, particularmente aos europeus, evidenciando um movimento de aproximação ao RGPD, que foi amplamente aceito como modelo de referência. No entanto, ao priorizar essa “harmonização” com os padrões globais, o processo legislativo falhou em desenvolver uma abordagem específica e profundamente enraizada na realidade social, econômica e cultural brasileira, o que compromete sua eficácia e sua legitimidade, conforme se verifica dos dados apresentados, em abundância, acerca dos abusos contra o direito de proteção aos dados pessoais dos brasileiros.

O percurso do projeto pela Câmara dos Deputados e Senado demonstrou uma preocupação excessiva em atender aos interesses econômicos internacionais, especialmente no que diz respeito a atrair investimentos de empresas de tecnologia e manter o Brasil competitivo no cenário global de negócios digitais. Esse objetivo, embora importante, criou uma tensão que afetou a essência do projeto de lei, desviando o foco da proteção de dados pessoais como um direito fundamental e aproximando-o mais de uma regulamentação voltada ao livre fluxo de informações para fins econômicos. A urgência com que foi aprovado, poucos dias antes da entrada em vigor do RGPD, também reflete uma reação quase automatizada, que pode ser vista como um indício da falta de profundidade no tratamento das necessidades locais e da independência regulatória brasileira.

Outro ponto de crítica ao processo legislativo da LGPD está na falta de um amplo debate público que realmente considerasse os interesses e as preocupações dos cidadãos brasileiros. As audiências realizadas focaram, em muitos casos, nos aspectos técnicos e nas exigências do mercado digital global, deixando de lado uma análise mais crítica sobre as implicações para a privacidade e a autonomia informacional. A LGPD, ao ser concebida rapidamente, foi pouco discutida com a sociedade civil e com especialistas em áreas como direitos humanos, filosofia da tecnologia e sociologia, o que poderia ter fornecido uma base mais rica para entender os impactos sociais e culturais da proteção de dados no Brasil. Esse vácuo de debate limitou a pluralidade de perspectivas e, em última análise, restringiu a capacidade da LGPD de endereçar as realidades específicas do Brasil.

Além disso, a influência econômica e política de corporações e governos estrangeiros no processo legislativo reforça a crítica de que a LGPD, embora essencial, ainda padece de um alinhamento com as dinâmicas de poder globais que privilegiam interesses do Norte Global sobre os do Sul. A pressão para que o Brasil adotasse padrões compatíveis com os do RGPD, sem adaptá-los completamente ao contexto nacional, reflete os fenômenos do neoliberalismo e do “colonialismo de dados”, no qual países do Sul Global acabam absorvendo modelos normativos que favorecem as potências econômicas. Esse cenário deixa o Brasil em uma posição de subserviência no mercado de dados globais, limitando sua capacidade de regular de maneira soberana e independente a proteção dos dados de seus cidadãos.

O fato de a LGPD ter sido inspirada no RGPD também traz à tona uma crítica quanto ao perigo da homogeneização normativa, que, embora benéfica em alguns aspectos, pode não ser adequada para países com realidades tecnológicas e socioeconômicas diferentes. O Brasil, como um país marcado por profundas desigualdades e desafios específicos no acesso e no uso de tecnologias, exige uma abordagem que leve em conta essas particularidades. A padronização de normas de proteção de dados, sem uma devida contextualização, compromete a capacidade da lei de atuar de maneira eficaz e de responder aos desafios locais. Em vez de uma legislação protetiva adaptada às necessidades brasileiras, o resultado foi uma norma que, em muitos aspectos, carece de mecanismos próprios para lidar com o contexto brasileiro de maneira efetiva.

Tanto a LGPD quanto o RGPD dispõem sobre a transferência internacional de dados, mas o fazem de maneiras que refletem as diferentes posições de poder e influência de suas respectivas jurisdições no cenário global. No caso do RGPD, a União Europeia estabelece critérios claros e rigorosos para a transferência de dados pessoais para países terceiros. A Comissão Europeia detém a competência para emitir decisões de adequação, que certificam se uma nação ou uma organização internacional oferece um nível de proteção adequado. Essa prerrogativa é exercida unilateralmente pela Comissão, consolidando a posição da União Europeia como um regulador global de proteção de dados, ao qual outras nações devem, de certa forma, se alinhar.

A LGPD, por outro lado, embora se inspire nesses critérios de adequação, enfrenta um contexto de vulnerabilidade e dependência, que enfraquece a autonomia brasileira. A ANPD, ao contrário da Comissão Europeia, não possui o mesmo grau de autonomia e força normativa para impor padrões de proteção adequados de forma independente. Ao abdicar de seu dever de emitir decisões de adequação com uma postura mais flexível e permissiva, a ANPD demonstra uma fragilidade que enfraquece a soberania informacional brasileira, abrindo espaço para que o país se submeta às exigências e interesses de agentes externos.

Esse cenário ressalta uma tensão fundamental na LGPD: enquanto, de um lado, a lei busca alinhar-se ao RGPD para facilitar o fluxo de dados entre Brasil e União Europeia, de outro, ela reflete uma adaptação insuficiente à realidade brasileira, que, ao não adotar uma postura assertiva, acaba permitindo que o fluxo internacional de dados se converta em uma via de exploração, mais do que de colaboração. Esse risco é exacerbado pela natureza voluntária das decisões de adequação conforme regulado pela Resolução CD/ANPD nº 19/2024. Em vez de se impor como um marco regulatório que protege a privacidade dos cidadãos contra o colonialismo de dados, a LGPD corre o risco de ser instrumentalizada para legitimar a transferência de dados ao exterior, sem a devida contrapartida de segurança e autonomia para o Brasil.

A estrutura e o texto da LGPD, portanto, sugerem que, mais do que atender aos interesses de proteção dos dados dos cidadãos brasileiros, sua implementação está profundamente vinculada a uma perspectiva econômica que coloca a proteção de dados como um facilitador do mercado global. A tentativa de inserir o Brasil no mercado digital global, ainda que importante para a economia, parece ter se sobreposto ao objetivo central de garantir uma proteção efetiva e autônoma para os dados pessoais dos brasileiros. Esse enfoque predominantemente econômico é um reflexo do neoliberalismo que permeia o cenário global, onde a privacidade e a proteção de dados são frequentemente vistas como secundárias frente aos interesses de mercado e ao livre fluxo de capital.

Diante disso, é imperativo que a ANPD reveja sua abordagem em relação à emissão de decisões de adequação, adotando critérios mais rigorosos e adaptados à realidade brasileira. É preciso que a agência reconheça a transferência internacional de dados não apenas como uma questão técnica ou econômica, mas como uma

questão de soberania e autonomia digital, essenciais para garantir que a LGPD se configure como um instrumento verdadeiramente protetivo e não como uma formalidade desprovida de substância. Essa mudança de perspectiva é crucial para que o Brasil possa, de fato, assegurar uma proteção de dados que atenda às necessidades e interesses de seus cidadãos, resistindo à pressão externa e ao colonialismo de dados, que transformam os dados pessoais em uma commodity a ser explorada por grandes corporações estrangeiras.

Em última análise, a LGPD precisa ser reinterpretada e implementada de maneira a fortalecer a autonomia brasileira no cenário digital global, estabelecendo salvaguardas robustas que permitam ao Brasil regular, de forma independente, a proteção dos dados pessoais de sua população. A ANPD, por sua vez, tem o dever de atuar como uma defensora ativa dessa autonomia, assegurando que o Brasil seja mais do que um mero executor das diretrizes internacionais, mas um protagonista na definição de suas próprias políticas de proteção de dados, alinhadas com as realidades locais e com a dignidade e privacidade de seus cidadãos.

Não apenas a LGPD, mas a legislação dela decorrente também deve ser – *in casu*, a Resolução CD/ANPD nº 19/2024 – severamente criticada: e aqui atingimos um ponto crucial de análise. A referida resolução, ao flexibilizar o processo de decisão de adequação, não apenas desconsidera o contexto específico de vulnerabilidades brasileiras no campo da proteção de dados, mas também subverte o próprio espírito protetivo da LGPD – talvez impensado pelo legislador ordinário, mas que, involuntariamente, consoante se verá, fornece, *distintamente* do que apregoa o RGPD, uma saída não apenas possível da submissão a que se refere a atual redação da Resolução, mas um dever epistêmico da ANPD.

Com efeito, a Resolução CD/ANPD nº 19/2024 sinaliza uma postura que prioriza os interesses comerciais e as pressões internacionais em detrimento da proteção robusta dos direitos fundamentais dos cidadãos brasileiros. Em vez de fortalecer a soberania informacional e a independência regulatória, a resolução transforma o país em um facilitador do fluxo de dados para grandes potências e corporações transnacionais, sem exigir garantias recíprocas de proteção. Dessa forma, a ANPD, por meio dessa Resolução, abdica de seu papel fundamental como defensora dos interesses nacionais e dos direitos dos cidadãos, permitindo uma

abertura perigosa para a exploração e manipulação de dados pessoais por agentes externos.

Ao abdicar da obrigatoriedade de decisões de adequação, a ANPD não apenas compromete a proteção dos dados dos cidadãos brasileiros, mas revela uma falta de compromisso real com a construção de uma soberania informacional robusta e autônoma. No contexto de um país como o Brasil, que ocupa uma posição periférica e subalterna no cenário global, essa postura regulatória permissiva alimenta um ciclo de dependência econômica e tecnológica que reduz a capacidade do Estado de proteger seus cidadãos contra a exploração indiscriminada de dados. Ao se recusar a adotar uma postura mais rigorosa e intransigente na avaliação dos países receptores de dados, a ANPD, por meio da resolução, abre mão de uma importante ferramenta de resistência ao neoliberalismo digital e ao colonialismo de dados, deixando as portas abertas para que potências estrangeiras e corporações transnacionais possam usufruir das informações dos brasileiros sem as devidas salvaguardas.

Ao instituir, portanto, a possibilidade de decisões de adequação de maneira facultativa, a resolução permite que a ANPD escolha não realizar uma análise rigorosa dos países receptores de dados pessoais brasileiros, o que fragiliza a proteção desses dados e expõe o Brasil a uma vulnerabilidade acrescida no cenário global. Em vez de assegurar uma posição firme e autônoma de controle, a resolução concede à ANPD um espaço de discricionariedade que pode ser facilmente moldado por pressões econômicas e políticas internacionais, promovendo uma flexibilização excessiva que contraria o princípio de proteção de dados como direito fundamental.

Esse ponto de crítica, diga-se mais uma vez, não é mero detalhe, pois a ausência de obrigatoriedade na análise de adequação perpetua uma postura regulatória passiva, onde o Brasil abre mão de seu potencial protetivo em favor de um alinhamento comercial assimétrico. A regulação normativa indica uma priorização do fluxo de dados com pouca reciprocidade real, o que afeta diretamente a segurança dos dados dos cidadãos brasileiros ao permitir que eles sejam tratados sob regimes legais que não oferecem as mesmas garantias que a LGPD, e mesmo que outras normas venham a prescrever. Nesse sentido, a resolução parece mais orientada a facilitar interesses de mercado do que a proteger os direitos de privacidade (aos

auspícios da LGPD), reforçando uma subordinação estrutural do Brasil às normativas e interesses externos, em mais uma confirmação do fenômeno do colonialismo de dados.

Assim, a Resolução CD/ANPD nº 19/2024 acaba refletindo uma visão regulatória neoliberal, que trata a proteção de dados não como um direito prioritário dos cidadãos, mas como um recurso a ser ajustado conforme demandas do mercado global. A decisão de adequação, sob a forma estabelecida pela Resolução, poderia ser um marco de resistência e proteção efetiva, assegurando que a transferência internacional de dados ocorresse apenas para países com um nível de proteção equivalente. Em vez disso, ao tratar essa avaliação como facultativa, a resolução fragiliza a soberania informacional e promove uma abertura arriscada aos interesses de agentes externos que podem explorar os dados brasileiros sob pretextos econômicos.

Essa postura crítica é fundamental para que o Brasil possa desenvolver um sistema de proteção de dados condizente com as exigências da democracia hoje vinculada, sem possibilidade de cisão, com seu Estado de Direito, superando a limitação de uma legislação voltada a tutelar os dados pessoais que, embora formalmente semelhante à europeia, falha em atender às particularidades do país e aos desafios enfrentados por uma nação do Sul Global.

Ao fim e ao cabo, a consolidação de uma política de dados *informacionalmente* soberana depende de um alinhamento estratégico entre a ANPD e o legislador brasileiro, que devem atuar conjuntamente para consolidar a LGPD e as demais normas que venham a compor o sistema de proteção de dados pessoais como um instrumento de proteção efetiva e não meramente simbólico. Isso implica, entre outras medidas, a revisão das cláusulas de adequação e das disposições de transferência internacional de dados, além da adoção de critérios rigorosos que impeçam o uso de dados brasileiros por agentes externos sem garantias de reciprocidade e segurança. A construção de uma soberania informacional passa, portanto, pela reafirmação de uma postura regulatória firme e independente, capaz de defender os interesses e a privacidade dos cidadãos brasileiros no contexto da economia digital global.

5 CONSIDERAÇÕES FINAIS: DESAFIOS E PERSPECTIVAS EMANCIPATÓRIAS – O NECESSÁRIO CONTROLE DE LEGALIDADE DO ART. 10 DA RESOLUÇÃO CD/ANPD Nº 19/2024

Os desafios e as perspectivas emancipatórias vão na esteira das reflexões realizadas no tópico anterior, e se fundamentam na compreensão de que a proteção de dados pessoais transcende a regulamentação técnica e se consolida como um pilar para o fortalecimento do Estado Democrático de Direito em um contexto global, onde o poder da informação cresce de maneira exponencial. Para que o Brasil se estabeleça de forma independente e proteja efetivamente seus cidadãos, a ANPD precisa adotar uma postura decididamente proativa, fundamentada nos princípios da LGPD e da Constituição Federal, que reconhecem a privacidade e a segurança dos dados como direitos fundamentais. Essa atuação é especialmente urgente diante das pressões externas que buscam, desde sempre, influenciar o controle dos dados brasileiros, minando a autonomia regulatória do país.

A construção de uma política de proteção de dados verdadeiramente emancipatória exige que o Brasil se posicione com firmeza diante das dinâmicas de exploração global representada pelo “colonialismo de dados” e pelas imposições neoliberais que frequentemente colocam o lucro acima dos direitos fundamentais e transformam os dados pessoais e a privacidade em mercadoria. Nessa perspectiva, a proteção dos dados pessoais deve ir além da adoção de normas estrangeiras, sendo desenvolvida com base nas necessidades e valores nacionais, com o compromisso de garantir a dignidade dos cidadãos e sua capacidade de decidir sobre o destino de suas informações pessoais. Essa abordagem marca uma linha de defesa essencial contra o uso descontrolado e o abuso de dados por grandes corporações e interesses externos, reafirmando o direito dos brasileiros à privacidade e ao controle sobre suas próprias informações.

Ao promover uma política informacional robusta e independente, a ANPD não apenas cumpre seu papel de autoridade reguladora, mas também atua como guardiã e defensora da democracia brasileira, garantindo que as informações pessoais dos cidadãos não sejam submetidas a uma lógica de exploração descontrolada e desprotegida. Ao proteger as informações pessoais de sua população, estabelece um

anteparo crucial contra o abuso de poder das grandes corporações e dos Estados centrais – o que depende de um alinhamento estratégico entre legislação, práticas regulatórias e um compromisso ético com o fortalecimento da autonomia nacional, de forma que o Brasil possa, em última análise, se projetar como um país verdadeiramente soberano, não apenas nas esferas política e econômica, mas também no domínio informacional, essencial para a proteção dos direitos fundamentais e para a consolidação de um espaço democrático analógico e digital.

Os dados pessoais não figuram apenas como efeitos colaterais necessários e indesejados das atividades econômicas contemporâneas, como se fossem “respingos” inevitáveis de um processo maior; ao contrário, são o próprio combustível que alimenta essa economia, constituindo a matéria-prima fundamental em torno da qual gravitam as atividades lucrativas de diversas atividades econômicas. Tornaram-se, portanto, insumos fundamentais para o funcionamento das economias modernas, em que a atividade lucrativa se alimenta do constante fluxo e exploração dos dados pessoais. Em uma sociedade digital, a captura e o tratamento de dados se configuram como etapas indispensáveis para a criação de valor, servindo de base para estratégias de mercado, inovação tecnológica e monitoramento comportamental. No entanto, essa exploração desmedida reforça uma estrutura econômica que privilegia a acumulação de informações em mãos privadas, em especial de grandes corporações globais, e também dos Estados ditos “centrais”, que controlam uma quantidade desproporcional de dados e, com isso, de poder. Assim, os dados deixam de ser simplesmente uma ferramenta auxiliar e passam a atuar como o próprio eixo do lucro, sustentando um sistema que frequentemente coloca em segundo plano a proteção de direitos individuais e a dignidade dos cidadãos.

Essa economia baseada na predação informacional não só transforma dados pessoais em mercadorias, mas também intensifica as desigualdades entre países e indivíduos, ampliando a vulnerabilidade das populações que, como no caso do Brasil, estão sujeitas a uma governança digital influenciada por interesses externos. A concentração de dados nas mãos de agentes econômicos poderosos reforça um novo tipo de colonialismo, onde as práticas de coleta e manipulação de dados de cidadãos de países periféricos favorecem majoritariamente as grandes potências e corporações multinacionais. Esse processo cria uma assimetria estrutural, em que os cidadãos e o

próprio Estado brasileiro têm pouca influência sobre o destino e o uso de suas informações, e onde a lógica do mercado frequentemente se sobrepõe ao compromisso ético de proteger a privacidade e a liberdade individual.

A situação se mostra ainda mais complexa e desafiadora quando o próprio Estado brasileiro, seja através de suas agências de segurança e inteligência, como a Abin, seja por meio de políticas públicas inadequadas, participa ou permite a coleta e análise indiscriminada de dados pessoais sob o pretexto de interesses de segurança ou desenvolvimento econômico. Essa atuação compromete não apenas a privacidade dos cidadãos, mas também solapa a confiança pública nas instituições, pois o Estado, ao replicar práticas de monitoramento e controle sem limites claros, se torna cúmplice do modelo de exploração informacional que deveria combater. Tal cenário agrava a vulnerabilidade dos brasileiros, que se veem expostos a uma dupla ameaça: a exploração de seus dados por corporações e potências estrangeiras e o risco de vigilância interna que muitas vezes ignora os limites constitucionais.

O colonialismo histórico foi embebido em exploração e violência física, cultural e psíquica das metrópoles contra as colônias; outrora, corpos periféricos masculinos e femininos de indígenas, negros e mestiços eram jogados na fogueira para nela, literalmente, arder como um *graveto oleoso*³⁴². Hoje, corpos periféricos da mesma natureza, somados a um recorte intenso de classe que atinge a imensa parte do povo brasileiro mestiço e multirracial, são condenados a uma existência indigna em razão da continuada exploração econômica em um contexto onde essa se moderniza e se torna mais sutil, mas se mantém igualmente opressiva. A condição de desigualdade permanece, ainda que os mecanismos de sua imposição e manutenção tenham adquirido nova roupagem.

Essa exploração moderna opera de maneira velada e eficiente, afastando-se da violência física explícita, mas impondo uma espécie de controle sutil sobre a vida das pessoas. As grandes corporações globais e os Estados hegemônicos impõem seus próprios interesses e agendas, coletando dados pessoais de indivíduos periféricos e transformando-os em mercadorias valiosas que são comercializadas e manipuladas sem qualquer retorno significativo para esses cidadãos. Nesse novo

³⁴² Expressão extraída de passagem emblemática de Ribeiro (1995, p. 92).

cenário, o colonialismo se manifesta através da privação de autonomia digital e do controle do fluxo informacional, processos que moldam o comportamento, limitam a liberdade de escolha e condicionam as oportunidades econômicas e sociais de maneira oculta, mas incisiva.

A luta pela emancipação digital e pelo controle efetivo dos dados pessoais precisa ser entendida como uma continuidade das lutas históricas por autonomia e dignidade. Assim como os movimentos de resistência buscaram, no passado, romper com a dominação colonial e a exploração econômica, hoje é imperativo que o Brasil e outros países periféricos estabeleçam mecanismos de proteção que garantam a seus cidadãos a plena posse e controle sobre suas informações. Essa é a nova fronteira da soberania nacional e da proteção dos direitos fundamentais, pois a liberdade digital e a autodeterminação informacional se tornaram essenciais para a dignidade humana e para a construção de uma democracia autêntica e inclusiva.

Confrontar o colonialismo de dados e suas ramificações — intensificadas pelo poder de controle sobre a privacidade e pelas dinâmicas neoliberais que transformam dados pessoais em mercadoria — com os princípios e garantias de um Estado Democrático de Direito não pode se limitar a um discurso vazio ou a uma retórica superficial. Esse enfrentamento exige um compromisso real e intransigente por parte do Estado e de suas instituições reguladoras, que devem tratar a proteção de dados como uma extensão concreta dos direitos fundamentais. E um compromisso real também dos juristas, em uma posição intransigível a favor do direito fundamental à proteção de dados pessoais. Isso significa que é imperativo que o discurso de defesa da privacidade e da autonomia e soberania informacionais se transforme em políticas efetivas e em uma regulamentação rígida, que resista às pressões de corporações e governos estrangeiros e que priorize os interesses da população brasileira. O discurso de um Estado comprometido com a dignidade e a autonomia de seus cidadãos, neste contexto, só terá legitimidade se houver um empenho em adotar uma postura vigilante e firme, que assegure que o fluxo informacional sirva aos interesses nacionais e respeite o direito dos cidadãos à privacidade e à autodeterminação.

Apostar em perspectivas emancipatórias significa colecionar atos de coragem. Há 60 anos, a coragem foi até o seu limite. Ir avante no caminho da resistência e independência poderia significar a luta armada, a guerra civil e a morte de brasileiras e brasileiros. A participação dos Estados Unidos, nesse contexto, esteve longe de ser ínfima³⁴³: quando o Golpe Civil-Militar finalmente se consolidou em 1964³⁴⁴, os Estados Unidos estavam prontos para intervir diretamente. O embaixador Lincoln Gordon agiu para que o presidente Lyndon Johnson reconhecesse rapidamente o novo governo militar e, caso fosse necessária, uma força militar americana estava em alerta para apoiar os golpistas no caso de uma guerra civil. No entanto, a resistência foi insuficiente para demandar uma intervenção desse porte, e os EUA logo começaram a negar qualquer envolvimento direto, enquanto financiavam grandes obras do regime militar e aumentavam a dívida externa brasileira. A influência estadunidense se estendeu para além do apoio econômico e técnico, pois a CIA também contribuiu para aprimorar os sistemas repressivos do governo brasileiro e de outras ditaduras latino-americanas³⁴⁵.

Vê-se, por exemplo, o que ocorreu no Chile, em 1973: o governo de Salvador Allende, legitimamente eleito e comprometido com reformas sociais e econômicas, foi brutalmente derrubado por um golpe militar, apoiado ativamente pelos Estados Unidos³⁴⁶. Nesse contexto violento, a Operação Condor, lançada em 1975, cumpriu

³⁴³ Ao contrário do que afirma, v.g. VILLA, 2014, p. 273.

³⁴⁴ Diversas ações, anteriores ao golpe, já buscavam impedir o avanço de supostos “ideais socialistas” no Brasil. Um exemplo foi a Aliança para o Progresso, implementada em 1961 para fortalecer a oposição ao governo de João Goulart. O projeto injetou capital em estados governados por adversários de Jango, como Carlos Lacerda, Magalhães Pinto e Ademar de Barros, com o objetivo de minar sua popularidade antes das eleições de 1965. Outras iniciativas incluíram o financiamento do Instituto Brasileiro de Ação Democrática (IBAD), responsável por campanhas anticomunistas veiculadas em cinemas, rádio e TV, e o apoio financeiro nas eleições parlamentares de 1962, com o intuito de eleger congressistas pró-EUA que pudessem se contrapor ao governo de Goulart. Além disso, o *soft power* dos EUA se manifestava em viagens com tudo pago para líderes brasileiros visitarem o país, reforçando uma visão favorável às políticas americanas. Esse conjunto de estratégias configurava uma tentativa clara de influência e controle, que buscava moldar o cenário político brasileiro à imagem dos interesses norte-americanos.

³⁴⁵ Sobre a participação dos Estados Unidos no Golpe Civil-Militar de 1964 e seu impacto subsequente: Fico, Carlos. **O Grande Irmão: da Operação Brother Sam aos Anos de Chumbo: o Governo dos Estados Unidos e a Ditadura Militar Brasileira** (Editora Civilização Brasileira, 2008); Green, James N. **Apesar de Vocês: a Oposição à Ditadura Militar de 1964 a 1985** (Companhia das Letras, 2009); Gaspari, Elio. **A Ditadura Envergonhada** (Companhia das Letras, 2002).

³⁴⁶ Com o medo de que o socialismo se consolidasse em mais um país da América Latina, a administração Nixon lançou mão de uma estratégia agressiva de desestabilização. Essa estratégia incluiu sabotagem econômica, financiamento de grupos de oposição e, finalmente, apoio direto ao golpe liderado pelo general Augusto Pinochet. As consequências foram devastadoras: um regime de repressão e violência sistemática se instalou, com milhares de chilenos mortos, desaparecidos e

um papel crucial como extensão das políticas estadunidenses na América Latina, institucionalizando uma rede repressiva transnacional entre os regimes militares do Cone Sul³⁴⁷.

Hoje, não porque dotado de maior ênfase em estratégias de coerção direta, mas envolto em uma sedução sofisticada e quase imperceptível, o controle se adapta aos tempos modernos, priorizando a adesão voluntária dos indivíduos a mecanismos de vigilância. Seduzidos pelo cântico da sereia neoliberal e pela ideologia que convence, muitos países periféricos e cidadãos que neles habitam entregam seus dados sem resistência, movidos pelas oportunidades econômicas e pelo desejo de visibilidade e reconhecimento nas redes digitais. Essa captação de informações ocorre por uma ambivalente conformidade, em um misto de imposição – sempre escamoteada de legalidade ou de genuína preocupação com a privacidade – e sedução: o atual modelo de coleta massiva é construído sobre o desejo de participação social, no qual as pessoas, movidas pela lógica do consumo e pela necessidade de aprovação, entregam espontaneamente informações pessoais para as empresas que dominam o cenário digital³⁴⁸, ao tempo que nações da periferia, a exemplo do Brasil, adaptam suas exigências normativas para que participem, com eficácia, desse mercado global.

torturados. Nesse sentido: FIORI, José Luís (org.). **Estados Unidos e a América Latina: A Construção da Hegemonia**. Petrópolis: Vozes, 2007; SCHITTINO, Renata. **Chile: o Golpe e o Impacto no Cone Sul**. Rio de Janeiro: Mauad X, 2013; GATTI, Vanessa Andreza. **Uma Nação Sob o Olhar de Washington: os Estados Unidos e o golpe de 1973 no Chile**. São Paulo: Editora Unesp, 2015.

³⁴⁷ A Operação Condor foi uma aliança secreta de cooperação entre as ditaduras militares da América do Sul, firmada nos anos 1970, com apoio direto dos Estados Unidos. Composta por países como Argentina, Chile, Uruguai, Paraguai, Bolívia e Brasil, seu objetivo era coordenar ações de repressão contra opositores políticos, especialmente aqueles identificados com movimentos de esquerda e de resistência aos regimes autoritários. A operação envolvia a troca de informações de inteligência, a captura e a transferência clandestina de pessoas entre fronteiras, além de práticas de tortura e desaparecimento forçado. Sob a justificativa de combate ao comunismo, a Operação Condor buscava eliminar qualquer ameaça ao status quo regional, criando um sistema transnacional de repressão que visava erradicar movimentos de resistência e consolidar o controle militar sobre a América Latina. Este acordo de cooperação transformou a região em um cenário de terror sistemático, onde violações aos direitos humanos ocorriam com impunidade, e onde o apoio dos EUA era fundamental para a formação e manutenção dessa rede de controle. A Operação Condor foi, assim, uma peça-chave na estratégia de interferência norte-americana, reforçando a dominação e impedindo tentativas de autonomia e democracia nos países envolvidos, cujos efeitos ressoam até hoje na memória política e social da América Latina. Nesse sentido: CUNHA, Luiz Cláudio. **A Operação Condor: Terrorismo de Estado no Cone Sul**. Porto Alegre: L&PM, 2008.

³⁴⁸ Sobre o assunto, ver: FALK, M.; SERBENA, C. A. Escopofilia virtual enquanto ideologia à luz de Marx E Engels. *In*: Pedro Paulo da Cunha Ferreira. (Org.). **Construindo Pontes: Diálogos entre Ciências Humanas e Sociais: v. 2., 1. ed.** São Paulo: Dialética, 2024, v. II, p. 301-324.

Esse contexto, que reflete o poder do colonialismo de dados, não ocorre de forma isolada. Ele é sustentado pela influência estratégica das potências centrais, como Estados Unidos e países europeus, que detêm o controle das principais plataformas e tecnologias de coleta de dados e orientam as práticas globais nesse setor. Com isso, o Brasil e outros países do Sul global veem-se inseridos em uma dinâmica de submissão, onde a lógica do mercado neoliberal transforma o próprio ato de ser visto em mercadoria e onde o "direito à privacidade" se dilui diante do império informacional das nações dominantes.

A decisão de adequação brasileira deve cumprir, portanto, um papel crucial nessa luta por emancipação, razão pela qual não deve ser o que hoje preceitua que seja o art. 10 da Resolução: uma faculdade da ANPD. Em vez de tratar a proteção de dados como um mero ajustamento às demandas do mercado global, a ANPD deve se tornar uma defensora intransigente dos direitos fundamentais dos cidadãos. Nesse contexto, a Resolução CD/ANPD nº 19/2024 precisa ser revisada para que a decisão de adequação seja tratada como um *dever obrigatório*, e não como uma faculdade. Apenas assim, o Brasil, em um contexto desproporcional de correlação de forças globais, poderá lutar para garantir que a transferência internacional de dados ocorra em condições de plena reciprocidade e respeito aos direitos individuais dos cidadãos.

Em relação ao tema da decisão de adequação, no que se refere à abordagem normativa, observa-se que o legislador caboclo, no afã de ser inglês, afastou-se da melhor técnica jurídica e acabou por estabelecer uma regulamentação que contradiz a própria Lei Geral de Proteção de Dados – criando uma brecha por meio da qual se pode afirmar uma perspectiva emancipatória frente aos desafios que a realidade concernente à transferência internacional de dados pessoais e sua correspondente necessidade de tutela nos impõe.

Diferentemente do que ocorre no Regulamento Geral de Proteção de Dados europeu, onde a emissão de decisões de adequação é tratada como uma faculdade normativa, na LGPD brasileira essa decisão é expressamente indicada como uma obrigação da Autoridade Nacional de Proteção de Dados no Capítulo V, que regula as transferências internacionais de dados.

Referida compreensão é extraída ao se compulsar o texto normativo da RGPD, mormente o contido no seu art. 45º, que utiliza verbos condicionais em sua

redação. Com efeito, referido artigo do RGPD) confere à Comissão Europeia a *possibilidade* de emitir decisões de adequação, mas não impõe um dever obrigatório de fazê-lo. Em outras palavras, o artigo estabelece que a transferência de dados pessoais para países terceiros ou organizações internacionais pode ocorrer se a Comissão Europeia decidir que esses locais garantem um nível adequado de proteção de dados. Contudo, essa decisão é uma *faculdade* da Comissão, ou seja, ela pode decidir realizar essa avaliação e emitir uma decisão de adequação, mas não é obrigada a fazê-lo.

Nesse sentido, o parágrafo 1 estabelece que a transferência de dados pessoais *pode* ser realizada se a Comissão decidir que há um nível adequado de proteção, o que implica que a decisão de adequação é opcional e fica a critério da Comissão Europeia. O parágrafo 2, por sua vez, fornece os elementos que a Comissão deve considerar ao avaliar a adequação, incluindo o respeito ao Estado de direito, Direitos Humanos e liberdades fundamentais no país ou organização destinatária, a existência de autoridades independentes para garantir o cumprimento das normas de proteção de dados, entre outros compromissos internacionais. No entanto, isso não obriga a Comissão a avaliar ou emitir uma decisão para cada país ou organização, apenas detalha os critérios caso a Comissão opte por fazê-lo. Por fim, segundo o parágrafo 3, a Comissão, após a avaliação, *pode* decidir, por meio de ato de execução, que um determinado país ou organização oferece proteção adequada. Mais uma vez, o verbo "*pode*" sugere uma escolha, não uma obrigação.

Assim, embora o artigo 45º permita à Comissão Europeia emitir decisões de adequação e forneça um quadro para avaliação, ele claramente trata essa ação como uma faculdade e não como uma obrigação. Isso significa que a Comissão Europeia tem discricionariedade para decidir em quais casos deseja realizar a avaliação e emitir uma decisão de adequação, e não está legalmente compelida a fazê-lo para cada país ou organização.

Os *Considerandos* do RGPD³⁴⁹ reforçam a interpretação de que a emissão de decisões de adequação pela Comissão Europeia é, de fato, uma faculdade, e não

³⁴⁹ Os Considerandos do Regulamento Geral de Proteção de Dados têm o papel de fornecer uma base interpretativa e contextual para as disposições do regulamento, mas não têm o mesmo estatuto normativo que seus artigos. Ugo Pagallo, por exemplo, explora o papel dos considerandos na interpretação e aplicação das normas do RGPD, destacando como eles fornecem diretrizes interpretativas que ajudam a contextualizar e operacionalizar os artigos do regulamento. Em termos

um dever. Eles trazem diversas disposições que reiteram a capacidade da Comissão de emitir tais decisões, mas sem estabelecer uma obrigatoriedade³⁵⁰.

Esses *Considerandos*, ao usarem, portanto, verbos permissivos para descrever as ações da Comissão, tornam claro que as decisões de adequação, a exemplo do que já esclarecem os artigos do RGPD, estão a critério da Comissão Europeia, não configurando um dever legal. Essa abordagem reflete o posicionamento europeu de manter uma flexibilidade regulatória, permitindo à Comissão Europeia decidir estrategicamente em quais casos e sob que circunstâncias realizar essa análise de adequação.

Diversa é a conclusão, no entanto, ao se interpretar o que prescreve a LGPD. A Lei Geral de Proteção de Dados brasileira, especialmente em seus artigos 33 e 34, utiliza uma linguagem normativa que estabelece um *dever* explícito para a Autoridade Nacional de Proteção de Dados de realizar a avaliação e a decisão de adequação em transferências internacionais de dados. Esse dever contrasta com a abordagem do

práticos, os considerandos não são vinculantes de forma autônoma como os artigos, ou seja, eles não têm força normativa direta para impor obrigações ou direitos. Servem, ainda, para clarificar o propósito e a intenção por trás das disposições específicas do RGPD, ajudando a contextualizar as normas e explicando o porquê de certas exigências, como no caso da proteção dos direitos fundamentais dos titulares de dados e da importância de um tratamento justo e transparente. Por fim, em situações de ambiguidade ou dúvida sobre o sentido de um artigo do RGPD, os considerandos podem ser usados como uma ferramenta de interpretação. Os tribunais e autoridades de proteção de dados frequentemente se referem aos considerandos para interpretar as disposições de maneira coerente com o espírito e os objetivos do regulamento. Nesse sentido: PAGALLO, Ugo. The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection. *Eur Law J.*, v. 24, n. 6, p. 533-555, 2018.

³⁵⁰ A análise dos seguintes *Considerandos* confirma essa interpretação: *Considerando 103* – A Comissão "pode decidir", com efeitos em toda a União, que um país ou organização internacional oferece um nível adequado de proteção. A escolha do verbo "pode" (em inglês, *may*) enfatiza que a emissão da decisão de adequação é uma possibilidade, não uma imposição. Aqui, a Comissão recebe o poder discricionário de avaliar e declarar adequação, o que permite transferências de dados sem autorização adicional. Contudo, o uso do verbo permissivo evidencia que tal avaliação ocorre a critério da Comissão, não sendo imposta; *Considerando 104* – Este Considerando expõe que a Comissão "deverá" considerar certos fatores ao avaliar a adequação de um país terceiro ou organização, como o respeito ao Estado de direito e aos direitos humanos. No entanto, ele apenas estabelece critérios para uma possível avaliação, não obriga a Comissão a realizá-la. Assim, o verbo "deverá" aparece para qualificar o modo de análise caso a Comissão decida exercer essa faculdade; *Considerando 106* – A Comissão "deverá" monitorar e revisar periodicamente a eficácia das decisões já emitidas sobre o nível de proteção de um país terceiro ou organização internacional. Essa obrigação de monitoramento aplica-se apenas uma vez que uma decisão de adequação tenha sido emitida. Assim, enquanto o monitoramento das decisões já existentes é obrigatório, a escolha inicial de emitir a decisão de adequação continua sendo uma opção; *Considerando 107* – Reitera que a Comissão "pode reconhecer" que um país ou organização deixou de assegurar um nível adequado de proteção e, nesse caso, deverá proibir a transferência de dados pessoais para esse país ou organização. Esse Considerando trata da capacidade da Comissão de revogar a decisão de adequação, mas novamente com o uso do verbo permissivo "pode", reforçando que a emissão ou revogação da decisão permanece discricionária.

Regulamento Geral de Proteção de Dados europeu, que trata a decisão de adequação como uma faculdade da Comissão Europeia.

Com efeito, o artigo 33 da LGPD restringe a transferência internacional de dados pessoais, permitindo-a apenas em situações específicas que garantam um nível de proteção adequado, alinhado ao previsto na lei. O inciso I especifica que a transferência *somente é permitida* para países ou organismos internacionais que proporcionem um *grau de proteção de dados pessoais adequado ao previsto nesta Lei*. Aqui, fica claro que a responsabilidade de garantir essa adequação está nas mãos da ANPD, já que não há liberdade irrestrita para transferências; ao contrário, essas devem se submeter ao requisito de proteção adequada.

No parágrafo único, a LGPD estabelece que órgãos públicos podem *requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional*. Isso demonstra que a LGPD prevê uma demanda por avaliações formais e conduzidas pela ANPD, reforçando sua responsabilidade nesse processo.

O artigo 34 da LGPD é ainda mais claro sobre o papel da ANPD na condução das avaliações de adequação, já que o texto do artigo usa o verbo “*será*” para descrever a responsabilidade da ANPD em avaliar o nível de proteção de dados do país estrangeiro ou organismo internacional. Ao dizer que o nível de proteção “*será avaliado*” pela ANPD, o texto não deixa margem para interpretação quanto à obrigatoriedade desse dever. Referido artigo lista, ainda, critérios que a ANPD *deve considerar* ao avaliar a adequação do nível de proteção de dados de países terceiros, como normas gerais e setoriais, natureza dos dados, princípios de proteção de dados e medidas de segurança. Essa listagem detalhada de requisitos evidencia uma metodologia de avaliação que a ANPD precisa seguir, conferindo caráter obrigatório ao processo.

Diante da redação dos artigos 33 e 34 da LGPD, é evidente que a ANPD possui, portanto, um dever legal de avaliar e decidir sobre a adequação dos países ou organizações internacionais em relação à proteção de dados para transferências internacionais. Esse caráter obrigatório destoa do RGPD, pois, enquanto o regulamento europeu apresenta a decisão de adequação como uma opção, a LGPD a coloca como uma responsabilidade intrínseca e essencial ao exercício da função

regulatória da ANPD. Assim, a ANPD deve realizar essa avaliação para garantir que as transferências internacionais respeitem o nível de proteção estabelecido pela legislação brasileira.

Repise-se referida conclusão: enquanto o RGPD, portanto, concede à Comissão Europeia a opção de emitir decisões de adequação, a LGPD estabelece claramente que a ANPD deve conduzir tais avaliações. No RGPD, o uso da palavra “*pode*” (em inglês, “*may*”) para indicar a emissão de decisões de adequação permite à Comissão a discricionariedade para escolher quando e como realizá-las. Já a LGPD, com termos como “*deve*” e “*será*”, não confere tal flexibilidade à ANPD, criando um cenário onde a autoridade nacional brasileira tem a obrigação normativa de assegurar a proteção adequada.

A distinção entre a legislação brasileira e a europeia quanto ao papel da autoridade reguladora, em maior e menor grau de discricionariedade para emitir decisões de adequação, pode ser interpretada de várias formas. A mais desejável, mas menos provável, parece ser aquela que conduziria ao fato dessa diferença normativa refletir uma resposta consciente e estratégica a desafios específicos do Brasil no cenário global, especialmente no que diz respeito ao colonialismo de dados e à vulnerabilidade de países do Sul Global em relação ao controle e uso de informações pessoais.

A mais provável e menos desejável, por sua vez, aponta para uma possível falta de atenção decorrente da pressa em adaptar normas internacionais ao contexto brasileiro, a fim de permitir a continuidade do fluxo internacional de dados pessoais entre a periferia e o centro, sem maiores adversidades econômicas para os atores interessados em ganhos políticos e financeiros.

Tal conclusão é apoiada pela redação que a ANPD conferiu à Resolução CD/ANPD nº 19/2024, mais especificamente em seu art. 10, por meio do qual procurou *flexibilizar* seu dever de emissão de decisões de adequação, ao dizer que **poderá**³⁵¹ *reconhecer, mediante decisão de adequação, a equivalência do nível de proteção de dados pessoais de país estrangeiro ou de organismo internacional com a legislação nacional de proteção de dados pessoais (...).*

³⁵¹ Grifos ausentes no original.

Ocorre que a Resolução, por sua natureza³⁵², é ato normativo *hierarquicamente inferior* ao texto normativo que busca explicitar – *in casu*, o disposto no Capítulo V da Lei Geral de Proteção de Dados. E mostra-se com ele incompatível, já que a LGPD, consoante visto alhures, cria uma obrigação normativa para que a ANPD assegure e reconheça, por meio da imperiosa decisão de adequação, a presença de um nível de proteção adequado para a transferência internacional de dados pessoais.

Aqui reside, portanto, a “brecha” mencionada anteriormente: ainda que de forma involuntária, a LGPD, enquanto parâmetro de qualquer Resolução editada ou por editar da ANPD, fixa-se como conteúdo mínimo e âncora normativa de qualquer norma sobre o assunto e que lhe seja inferior hierarquicamente, solidificando o dever de adequação como obrigatório e não como uma mera escolha administrativa. Esse posicionamento, ao arrepio dos que se beneficiam da flexibilidade na transferência de dados pessoais em caráter transnacional, pode e deve ser aproveitado como uma postura de resistência e de afirmação da soberania informacional e analógica do país.

Do confronto entre normas hierarquicamente desiguais e incompatíveis, forçoso se mostra a análise do tema relacionado ao estudo das *normas de estrutura*, mais especificamente, das *normas de eliminação jurídica*.

Nesse aspecto, Adrian Sgarbi nos ensina que as normas de eliminação jurídica têm a função de retirar normas do ordenamento jurídico, atuando de forma

³⁵² No Direito brasileiro, uma resolução é um ato normativo administrativo, normalmente emanado de órgãos colegiados, como conselhos, comissões e agências reguladoras, e também de casas legislativas (Senado e Câmara dos Deputados) para disciplinar questões internas ou regulamentar matérias específicas. A natureza jurídica de uma resolução é, em regra, infralegal e complementar, pois visa regulamentar normas previamente estabelecidas em leis e não tem, portanto, força de lei. A Constituição Federal e o Regimento Interno de cada órgão definem a competência para a emissão de resoluções. Em nível legislativo, a Constituição Federal prevê que o Congresso Nacional, o Senado e a Câmara dos Deputados possam editar resoluções para matérias específicas, como a aprovação de tratados internacionais (art. 49) e questões orçamentárias e de finanças (art. 52). Além disso, cada casa legislativa e entidade pública possui um regimento interno que regula o processo de elaboração de resoluções, detalhando as competências dos órgãos colegiados e o procedimento interno. Em relação às agências reguladoras e outros órgãos administrativos, a competência para editar resoluções encontra-se nos próprios regimentos internos de cada agência, previstos por lei específica que confere poder normativo para regulamentar temas dentro de sua competência. Há, ainda, a previsão na própria Lei das Agências Reguladoras (Lei nº 13.848/2019), que estabelece normas gerais para o funcionamento das agências e garante poder normativo para detalhar disposições legais que regulamentam o setor regulado. Portanto, a resolução é um ato normativo cuja autoridade e alcance dependem do órgão que a emite e do âmbito da matéria que regulamenta. Em todos os casos, as resoluções devem respeitar a hierarquia jurídica, posicionando-se como instrumentos de execução de normas e complementação das leis. Sobre o assunto: (CARVALHO FILHO, 2021, p. 123-125).

contrária às normas de criação jurídica. Elas são essenciais para manter o sistema jurídico atualizado e livre de normas obsoletas ou incorretas³⁵³.

De acordo com o autor, existem duas formas principais de eliminação jurídica: a *revogação* e a *nulificação*. A *revogação* é o processo pelo qual uma autoridade normativa, normalmente o legislador, elimina uma norma jurídica existente, seja em caráter geral ou específico³⁵⁴.

A *nulificação*, por sua vez, se refere à eliminação de normas que foram produzidas de forma irregular ou que violam normas hierarquicamente superiores. Diferente da revogação, que é um ato regular e planejado, a nulificação ocorre quando uma norma é considerada inválida devido a vícios em sua criação.

A *nulificação* pode se dar forma absoluta ou relativa³⁵⁵, e existem diferentes tipos de controle para a nulificação, destacando-se: o *controle de constitucionalidade* (quando a norma viola a Constituição); o *controle de convencionalidade* (quando a norma contraria tratados internacionais); e o *controle de legalidade* (quando a norma infringe outras normas legais inferiores à Constituição)³⁵⁶.

Embora tanto a revogação quanto a nulificação resultem na eliminação de normas, elas diferem em vários aspectos, já que, a um, a revogação é um ato regular realizado por uma autoridade competente, enquanto a nulificação decorre de irregularidades na criação da norma; a dois, a revogação segue os procedimentos legais, mantendo a fidelidade ao ordenamento jurídico, enquanto a nulificação ocorre por infidelidade às normas hierarquicamente superiores; a três, a revogação visa

³⁵³ Consoante leciona Sgarbi: “Normas de eliminação jurídica” são normas que participam da dinâmica jurídica cumprindo a função de “excluir” os materiais jurídicos. Não são normas de “ingresso”, mas normas de “egresso” normativo. Portanto, exercem função contrária às normas sobre a “criação jurídica”. SGARBI, 2021, p. 61.

³⁵⁴ Sgarbi indica que a revogação pode ser *geral*, quando uma norma nova revoga todas as normas anteriores que conflitam com ela; ou *específica*, quando uma norma específica é revogada por outra norma específica. Além disso, é importante não confundir a revogação como ato (o processo de eliminar a norma) com os efeitos da revogação (a consequência de que a norma não tem mais validade). Além disso, a revogação deve seguir os procedimentos legais estabelecidos para garantir sua validade. Nesse sentido: Sgarbi (2021, p. 61-62).

³⁵⁵ Adrian Sgarbi ensina que: “ser preciso aqui é relevante, pois em caso de nulificação absoluta, a regra é que tudo que foi produzido sob a sua regência é destruído desde a origem. Com respeito à relativa, o ato pode ser corrigido ou aproveitado de muitas maneiras. Ou seja, o legislador pode prever peculiaridades para cada ato de nulificação. Pense-se aqui na ‘modulação de efeitos’ no controle de constitucionalidade, como também na preservação de atos normativos em razão da ‘segurança jurídica’, do princípio da ‘confiança’, da ‘não-surpresa’, do ‘aproveitamento’, ou da ‘aparência’”. (SGARBI, 2021, p. 62-63).

³⁵⁶ *Idem*.

modificar ou atualizar o ordenamento jurídico, enquanto a nulificação busca preservar a integridade do sistema jurídico, eliminando irregularidades; e, a quatro, a revogação envolve a preferência temporal entre normas, enquanto a nulificação está relacionada à hierarquia das normas, priorizando normas superiores sobre as inferiores³⁵⁷.

Pois bem. No caso em tela, aplicando-se a inteligência da Teoria do Direito ao confronto entre o que dispõem os art. 33, I, e art. 34, *caput*, da LGPD, com o que prescreve o art. 10 da Resolução CD/ANPD nº 19/2024, constata-se que há uma clara violação da hierarquia normativa. Nesse embate, o princípio da supremacia da lei se impõe, pois a Resolução, enquanto ato administrativo normativo, deve necessariamente estar em conformidade com a LGPD, que é uma lei ordinária e, portanto, hierarquicamente superior. A Resolução não pode criar uma discricionariedade onde a lei expressamente impõe um dever³⁵⁸.

Assim, à luz das normas de eliminação jurídica expostas, assim como *quando um contrato civil não atende certa exigência do Código Civil, diz-se que é necessário controlar a legalidade do contrato*³⁵⁹, o art. 10 da Resolução pode – em verdade, *deve* – ser alvo de nulificação por violar diretamente a LGPD. Este dispositivo tenta transformar o dever de reconhecimento de adequação, previsto na lei, em uma faculdade, o que gera uma incompatibilidade jurídica essencial que compromete a validade desse artigo. Nesse sentido, a nulificação se apresenta como o mecanismo mais adequado para corrigir essa irregularidade normativa e preservar a integridade do ordenamento jurídico.

Ao redigir a Lei Geral de Proteção de Dados brasileira sem recorrer aos verbos condicionais³⁶⁰ empregados pelo RGPD europeu, e internalizar o dever de

³⁵⁷ *Idem*.

³⁵⁸ Em tese, o art. 10 da Resolução CD/ANPD nº 19/2024, ao conferir caráter facultativo à emissão de decisões de adequação pela ANPD, poderia ser alvo, inclusive, de controle de constitucionalidade. Isso porque a Resolução, ao contradizer os arts. 33 e 34 da LGPD, acaba por comprometer a eficácia do direito fundamental à proteção de dados pessoais, consagrado no art. 5º, inciso LXXIX, da Constituição Federal. Ao flexibilizar uma obrigação normativa que visa proteger a privacidade e a segurança dos dados, a Resolução enfraquece o regime constitucional de tutela de direitos fundamentais e afronta o princípio da legalidade. Sendo assim, o controle de constitucionalidade se justifica como uma medida adequada para preservar a supremacia da Constituição e garantir que normas infralegais, como resoluções administrativas, respeitem os limites e diretrizes estabelecidos pela lei e pela Carta Magna, assegurando, em última análise, a efetiva proteção dos direitos dos cidadãos.

³⁵⁹ SGARBI, 2021, p. 62.

³⁶⁰ Verbos condicionais são aqueles que expressam possibilidade, opção ou potencialidade, geralmente indicando que uma ação ou estado depende de uma condição para ocorrer. Eles são comumente utilizados para transmitir uma ideia de incerteza, permissão ou intenção condicionada.

adequação diretamente nos textos normativos da LGPD, o legislador brasileiro pode ter consolidado uma oportunidade de grande relevância: ao invés de um alinhamento superficial, criou-se para a ANPD, voluntária ou involuntariamente, um dever normativo real de proteger ativamente os dados dos brasileiros nas transferências internacionais. Esse dever se coloca, portanto, como um instrumento de emancipação e resistência frente ao colonialismo de dados e ao modelo neoliberal que frequentemente instrumentaliza a privacidade como recurso econômico.

Essa suposta "confusão" normativa revela-se, em última análise, como um trunfo inesperado, que, se bem utilizado, pode permitir que o Brasil se imponha no cenário internacional. Ao agir com coragem e firmeza, cumprindo seu papel de reguladora obrigatória e intransigente, a ANPD pode não só assegurar um elevado padrão de proteção de dados, mas também tornar-se um exemplo de resistência ao poder econômico das potências centrais. Dessa forma, a ANPD, longe de adotar a abordagem permissiva e flexível do RGPD, não apenas respeitaria sua própria estrutura normativa, mas também fortaleceria a autonomia regulatória nacional frente às pressões globais. Essa postura, longe de ser meramente técnica, representa uma escolha política e ética pela soberania, essencial para a proteção dos direitos fundamentais e para a afirmação de um Estado Democrático de Direito que valoriza a dignidade e a privacidade de seus cidadãos.

A implementação de uma normativa voltada à tutela dos dados pessoais com vocação verdadeiramente soberana deve ir além, ainda, da simples proteção contra abusos e vigilância; ela precisa fomentar uma sociedade mais justa e inclusiva, na qual todos os cidadãos brasileiros, especialmente os mais vulneráveis, possam usufruir dos avanços tecnológicos sem comprometer sua privacidade e autonomia. Ao se comprometer com essa causa e reconhecer a *ilegalidade* do disposto na Resolução CD/ANPD nº 19/2024 acerca da suposta faculdade de se emitir "decisões de adequação" quanto a transferência internacional de dados pessoais, a ANPD se posicionaria não apenas como uma entidade reguladora, mas como uma guardiã da democracia e da liberdade no ambiente digital, assegurando que o Brasil exerça um protagonismo ético e firme na proteção dos direitos fundamentais em tempos de intensa transformação digital.

REFERÊNCIAS

- ABBAGNANO, Nicola. Dicionário de Filosofia. Tradução de Alfredo Bosi. 4. ed. São Paulo: Martins Fontes, 2007.
- AIETA, Vânia Siciliano. Marco Civil da Internet e o Direito à Intimidade. *In*: LEITE, George Salomão; LEMOS, Ronaldo (coords). **Marco Civil da Internet**. São Paulo: Atlas, 2014, p. 695-710.
- AIETA, Vânia Siciliano. A necessária distinção entre demos e Kratos - poder do povo ou poder sobre o povo? Quem é o Povo? A Titularidade do Poder Constituinte Originário, **Revista Justiça Eleitoral em Debate**, v. 6, p. 16-27, 2016.
- ALMEIDA, Daniel F. P. S. de. A proteção de dados pessoais: uma análise da LGPD. **Revista Brasileira de Direito Digital**, v. 10, n. 1, 2020; MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. Comentários ao GDPR. 2. ed. São Paulo: Thomson Reuters Brasil, 2019
- ANDRADE, F. S. **Da Codificação**: Crônica de um Conceito. Porto Alegre: Livraria dos Advogados, 1997. v. 1. 189 p.
- ARRIGHI, Giovanni. **O longo século XX**: dinheiro, poder e as origens de nosso tempo. Rio de Janeiro: Contraponto Editora, 2007.
- ATIENZA, Manuel. **O Direito como Argumentação**. Tradução de Maria Cristina Guimarães Cupertino. Rio de Janeiro: Forense, 2014.
- AVELINO, Rodolfo da Silva. **Colonialismo Digital**: Dimensões da Colonialidade nas Grandes Plataformas.
- BABONES, Salvatore J. The Country-level Income Structure of the World-economy. **Journal Of World-Systems Research**, 11(1):29–55, 2005.
- BARROSO, Luís Roberto. **Curso de Direito Constitucional contemporâneo**: os conceitos fundamentais e a construção do novo modelo. 7. ed. São Paulo: Saraiva Educação, 2018.
- BARROSO, Luís Roberto. Revolução tecnológica, crise da democracia e mudança climática: limites do direito num mundo em transformação, *Journal of Institutional Studies* 3 (2019), **Revista Estudos Institucionais**, v. 5, n. 3, p. 1262-1313, set./dez. 2019.
- BATISTA, Mateus Mabelini; CARNUT, Leonardo; MENDES, Áquilas Nogueira. **O Consenso de Washington, vulnerabilidade externa e a superexploração do trabalho na América Latina: uma análise à luz da Teoria Marxista da**

Dependência. De Raíz Diversa: **Revista Especializada em Estudos Latino Americanos**, v. 8, n. 15, 2021, p. 73-109.

BAUMAN, Zygmunt. **Globalização: As consequências humanas.**

BAUMAN, Zygmunt. **A arte da vida.** Rio de Janeiro: Zahar, 2009.

BAUMAN, Zygmunt. **O mal-estar da pós-modernidade.** Rio de Janeiro: Zahar, 2012.

BAUMAN, Zygmunt. **Em Busca da Política.** Rio de Janeiro: Zahar, 2000.

BAUMAN, Zygmunt. **Globalização: as consequências humanas.** Rio de Janeiro: Zahar, 1999.

BAUMAN, Zygmunt. **Legisladores e Intérpretes: sobre modernidade, pós-modernidade e intelectuais.** Rio de Janeiro: Zahar, 2010.

BAUMAN, Zygmunt. **Modernidade e Holocausto.** Rio de Janeiro: Zahar, 1998.

BAUMAN, Zygmunt. **Modernidade Líquida.** Rio de Janeiro: Zahar, 2001.

BAUMAN, Zygmunt. **Modernidade e Ambivalência.** Rio de Janeiro: Jorge Zahar, 1999.

BAUMAN, Zygmunt. **Por uma Sociologia Crítica: um ensaio sobre senso comum e emancipação.** Rio de Janeiro: Zahar, 1977.

BAUMAN, Zygmunt. **Tempos Líquidos.** Rio de Janeiro: Zahar, 2007.

BAUMAN, Zygmunt. **Vigilância Líquida: diálogos com David Lyon.** Rio de Janeiro: Zahar, 2014.

BAUMAN, Zygmunt. **Cegueira moral: a perda da sensibilidade na modernidade líquida.** Rio de Janeiro: Zahar, 2014.

BAUMAN, Zygmunt. **A ética é possível num mundo de consumidores?** Rio de Janeiro: Zahar, 2011.

BAUMAN, Zygmunt. **Capitalismo Parasitário.** Tradução Eliana Aguiar. Rio de Janeiro: Zahar, 2010.

BAUMAN, Zygmunt. **A sociedade individualizada: vidas contadas e histórias vividas.** Tradução José Gradel. Rio de Janeiro: Zahar, 2008.

BAUMAN, Zygmunt. **Vida a crédito: conversas com Citlali Rovisrosa-Madrado.** Tradução Alexandre Werneck. Rio de Janeiro: Zahar, 2010.

BAUMAN, Zygmunt, MAURO, Ezio. **Babel: entre a incerteza e a esperança**. Tradução Renato Aguiar. Rio de Janeiro: Zahar, 2016.

BBC News Mundo. **La falta de privacidad apoya un sistema económico inmoral, asegura filósofa mexicana**. Disponível em: <https://abrir.link/Ra1HS>. Acesso em: 15 set. 2023.

BENTHAM, Jeremy. **O Panóptico**. Belo Horizonte: Autêntica, 2008.

BIONI, Bruno Ricardo. **Privacidade no Século 21: Proteção de Dados, Democracia e Modelos Regulatórios**. Revista Brasileira de Ciência Política, n. 41, 2023.

BIONI, Bruno Ricardo. **Xeque-mate: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo, 2015. [Recurso em meio eletrônico].

BIZZARRO, FERNANDO; COPPEDGE, MICHAEL. **Variedades da Democracia no Brasil**. Opinião Pública (UNICAMP), v. 23, p. 1-42, 2017.

BLACK, Edwin. **IBM e o Holocausto: a aliança estratégica entre a Alemanha nazista e a mais poderosa empresa americana**. Tradução de Marcos Santarrita. Rio de Janeiro: Imago, 2001.

BOBBIO, Norberto. **Liberalismo e Democracia**. Tradutor Marco Aurélio Nogueira, Edipro, 2017.

BOBBIO, Norberto. **Teoria do Direito**. Tradução de Denise A. Campos. 4. ed. São Paulo: Editora Martins Fontes, 2010.

BOLZAN DE MORAIS, José Luis; MENEZES NETO, Elias Jacob de. **Direitos Fundamentais e Surveillance: as antidemocráticas e assimétricas relações de visibilidade possibilitadas pela tecnologia da informação**. In: CONPEDI/UNICURITIBA (Org.). Direito e Novas Tecnologias. Florianópolis: FUNJAB, 2013.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF, Senado, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constitui%C3%A7ao.htm. Acesso em: 02 mar. 2017.

BRASIL. **Lei n. 12.414, de 09 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm. Acesso em: 02 mar. 2017.

BRASIL. **Lei n. 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 02 mar. 2017.

BRASIL. **Lei n. 12.654, de 28 de maio de 2012.** Altera as Leis nos 12.037, de 1º de outubro de 2009, e 7.210, de 11 de julho de 1984 - Lei de Execução Penal, para prever a coleta de perfil genético como forma de identificação criminal, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12654.htm. Acesso em: 02 mar. 2017.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 02 mar. 2017.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 ago. 2023.

BRASIL. **Lei n. 7.232, de 29 de outubro de 1984.** Dispõe sobre a Política Nacional de Informática, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L7232.htm. Acesso em: 02 mar. 2017.

BRASIL. **Lei n. 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8078.htm. Acesso em: 02 mar. 2017.

BRASIL. **Decreto-Lei n. 2.848, de 07 de dezembro de 1940.** Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/De12848compilado.htm. Acesso em: 02 mar. 2017.

BUTLER, Judith. **Notas para uma teoria performativa da assembleia.** Tradução de Rogério Bettoni. São Paulo: Civilização Brasileira, 2019

CÂMARA DOS DEPUTADOS. Comissão Especial destinada a proferir parecer ao Projeto De Lei nº 4060, de 2012 (Tratamento e Proteção de Dados Pessoais). **Projeto de Lei nº 4.060, de 2012.** (Apenso PLs nº 5.276/16 e 6.291/16). Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: https://camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filena me=Tramitacao-PL%204060/2012. Acesso em: 06 ago. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 4.060, de 2012.** Dispõe sobre o tratamento e proteção de dados pessoais. Relator: Deputado Orlando Silva. P. 2-4. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=PRL%201%20PL406012%20=%3E%20PL%204060/2012. Acesso em: 06 ago. 2023.

CÂMARA DOS DEPUTADOS. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1006079&filename=Tramitacao-PL%204060/2012. Acesso em: 04 ago. 2023.

CÂMARA DOS DEPUTADOS. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1665276&filename=Tramitacao-PL%204060/2012. Acesso em: 07 ago. 2023.

CÂMARA DOS DEPUTADOS. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1664774&filename=Tramitacao-PL%204060/2012. Acesso em 07 ago. 2023.

CÂMARA DOS DEPUTADOS. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750&filename=Tramitacao-PL%204060/2012. Acesso em: 04 ago. 2023.

CÂMARA DOS DEPUTADOS. **Requerimento nº, de 2015. do Sr. Sérgio Zveiter.** Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1330147&filename=Tramitacao-PL%204060/2012. Acesso em: 04 ago. 2023.

CÂMARA DOS DEPUTADOS. Comissão de Ciência e Tecnologia, Comunicação e Informática. **Projeto de Lei nº 4060, de 2012.** Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1454623&filename=Tramitacao-PL%204060/2012. Acesso em: 05 ago. 2023.

CÂMARA DOS DEPUTADOS. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1501981&filename=Tramitacao-PL%204060/2012. Acesso em: 05 ago. 2023.

CÂMARA DOS DEPUTADOS. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1509440&filename=Tramitacao-PL%204060/2012. Acesso em: 05 ago. 2023.

CÂMARA DOS DEPUTADOS. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1509235&filename=Tramitacao-PL%204060/2012. Acesso em: 05 ago. 2023.

CÂMARA DOS DEPUTADOS. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1517227&filename=Tramitacao-PL%204060/2012. Acesso em 05 ago. 2023.

CÂMARA DOS DEPUTADOS. https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=Tramitacao-PL%204060/2012. Acesso em: 08 ago. 2023.

CÂMARA DOS DEPUTADOS. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=Tramitacao-PL%204060/2012. Acesso em: 08 ago. 2023.

CANAL TECH. **Após bloqueio no Brasil, CEO do Telegram pede desculpas ao STF por negligência.** Disponível em: <https://canaltech.com.br/juridico/apos-bloqueio-no-brasil-ceo-do-telegram-pede-desculpas-ao-stf-por-negligencia-211942/>. Acesso em: 20 ago. 2023.

CANAL TECH. **Vazamento expõe quase 6 milhões de dados de saúde dos brasileiros.** Disponível em: <https://canaltech.com.br/seguranca/vazamento-expoe-quase-6-milhoes-de-dados-de-saude-dos-brasileiros-246314/>. Acesso em: 21 ago. 2023.

CANAL TECH. **10 milhões de brasileiros têm dados vazados todos os meses.** Disponível em: <https://canaltech.com.br/seguranca/10-milhoes-de-brasileiros-tem-dados-vazados-todos-os-meses-254304/>. Acesso em: 21 ago. 2023.

CANAL TECH. **Brasil foi o país com mais credenciais vazadas em 2022.** Disponível em: <https://canaltech.com.br/seguranca/brasil-foi-o-pais-com-mais-credenciais-vazadas-em-2022-249474/>. Acesso em: 21 ago. 2023.

CANOTILHO, José Joaquim Gomes. **Direito Constitucional e Teoria da Constituição.** 7. ed. Coimbra: Livraria Almedina, 2003.

CARDOSO, Fernando Henrique e Weffort, Francisco (eds.) **América Latina.** Ensayos de interpretación sociológica (Santiago do Chile: Editorial Universitaria.

CARVALHO FILHO, José dos Santos. **Manual de Direito Administrativo.** 34. ed. São Paulo: Atlas, 2021.

CASALECCHI, Gabriel Ávila. **Legado Democrático e Apoio à Democracia na América Latina: Evidências e Mecanismos Explicativos**. Curitiba: Editora UFPR, 2018.

CASSINO, João Francisco; SILVEIRA, Sérgio Amadeu da; SOUZA, Joyce; **Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal**. São Paulo: Autonomia Literária, 2021.

CASTRO, Catarina Sarmiento e. **Direito da informática, privacidade e dados pessoais**: a propósito da legalização de tratamentos de dados pessoais (incluindo videovigilância, telecomunicações e Internet) por entidades públicas e por entidades privadas, e da sua comunicação e acesso. Coimbra: Almedina, 2005.

CHAUÍ, Marilena. **Democracia: criação de direitos**. Síntese: Revista de Filosofia, Belo Horizonte, v. 45, n. 143, p. 409-422, set./dez., 2018.

COLLIER, David; LEVITSKY, Steven. **Democracy with Adjectives: Conceptual Innovation in Comparative Research**. World Politics, v. 49, n. 3, p. 430-451, 1997.

COMITÊ GESTOR DA INTERNET NO BRASIL. **14º Seminário de Proteção à Privacidade e aos Dados Pessoais**. Disponível em: <https://seminarioprivacidade.cgi.br/>. Acesso em: 08 ago. 2023.

CONJUR. **Petição 9.935**, Distrito Federal. <https://www.conjur.com.br/dl/alexandre-moraes-ordena-bloqueio.pdf>. Acesso em: 20 ago. 2023.

CONSULTOR JURÍDICO. **STF vai julgar em sessão presencial se WhatsApp pode ser suspenso pela Justiça**. <https://www.conjur.com.br/2023-set-26/stf-julgar-whatsapp-suspenso-ordem-judicial>. Acesso em: 20 ago. 2023.

CONVENÇÃO AMERICANA SOBRE DIREITOS HUMANOS, 1969. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm. Acesso em: 10 mar. 2017.

COULDRY, Nick; MEJIAS, Ulises. **Data Grab: The New Colonialism of Big Tech and How to Fight Back**, Penguin Random House and University of Chicago Press, 2019. [Recurso em meio eletrônico].

COULDRY, Nick; MEJIAS, Ulisses A. **The costs of connection**: how data is colonizing human life and appropriating it for capitalism. Stanford University Press, 2019.

CUNHA, Luiz Cláudio. **A Operação Condor: Terrorismo de Estado no Cone Sul**. Porto Alegre: L&PM, 2008.

CUPANI, Alberto. **Filosofia da tecnologia**: um convite. 3. ed. Florianópolis: Editora da UFSC, 2016.

CURY, Paula Maria Nasser. **Métodos de Direito Comparado: desenvolvimento ao longo do século XX e perspectivas contemporâneas**. Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD), v. 6, n. 2, p. 176-185, 2014.

DALAQUA, Gustavo Hessmann. Democracia e verdade: uma defesa contingente da democracia epistêmica. **Revista Brasileira de Ciência Política**, n. 22. Brasília, jan. abr. 2017, p 191-232.

DANA, Samy. Ashley Madison: o que a economia nos diz sobre a traição. **JP News**. <https://jovempan.com.br/arquivo/samy-dana/ashley-madison-o-que-a-economia-nos-diz-sobre-a-traicao.html>. Acesso em: 20 ago. 2023.

DANTAS, Thaile. Netshoes terá de pagar R\$ 500 mil por vazamento de dados de milhões de clientes. **JusBrasil**. Disponível em: <https://www.jusbrasil.com.br/noticias/netshoes-tera-de-pagar-r-500-mil-por-vazamento-de-dados-de-milhoes-de-clientes/685006882>. Acesso em: 20 ago. 2023.

DE RUGGIERO, Guido. **Storia del liberalismo europeo**. Bari: Laterza, 1925.

DECLARAÇÃO AMERICANA DOS DIREITOS E DEVERES DO HOMEM, 1948. Disponível em: https://www.cidh.oas.org/basicos/portugues/b.Declaracao_Americana.htm. Acesso em: 10 mar. 2017.

DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS, 1948. Disponível em: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/por.pdf. Acesso em: 10 mar. 2017.

DIÁRIO DA CÂMARA DOS DEPUTADOS. Disponível em: <https://imagem.camara.gov.br/Imagem/d/pdf/DCD14JUN2012.pdf#page=212>. Acesso em: 04 ago. 2023.

DIMOULIS, Dimitri. **Manual de introdução ao estudo do direito**. São Paulo: Revista dos Tribunais, 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. **Novas faces do poder no mundo digital**. Disponível em: <https://doneda.net/novas-faces-do-poder-no-mundo-digital/>. Acesso em: 04 ago. 2023.

DONEDA, Danilo. Risco e Informação Pessoal: o Princípio da Finalidade e a Proteção de Dados no Ordenamento Brasileiro. **R. Bras. Risco e Seg.**, Rio de Janeiro, v. 5, n. 10, p. 85-102, out. 2009/mar. 2010 85. Disponível em: <https://www.rbrs.com.br/arquivos/RBRS10-4%20Danilo%20Doneda.pdf>. Acesso em: 04 ago. 2023.

EL PAÍS. “**Me han robado la identidad y estoy a base de lexatín; yo no soy un delincuente**”. Publicado em 24 de agosto de 2016. Disponível em: https://elpais.com/politica/2016/08/23/actualidad/1471908298_138488.html. Acesso em: 20 ago. 2023.

EUROPEAN UNION. **RGPD**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 15 ago. 2023.

FALK, Matheus. **A necessidade de proteção aos dados pessoais no direito brasileiro**: tutela jurídica na era da modernidade líquida e da surveillance. Dissertação (Mestrado em Direito) – Universidade Federal do Paraná, Curitiba, 2017.

FALK, Matheus.; SERBENA, C. A. Escopofilia virtual enquanto ideologia à luz de Marx e Engels. *In*: FERREIRA, Pedro Paulo da Cunha. (Org.). **Construindo Pontes**: Diálogos entre Ciências Humanas e Sociais. 1. ed., São Paulo: Dialética, 2024, v. II.

FEENBERG, Andrew. **Entre a razão e a experiência: ensaios sobre tecnologia e modernidade**. Tradução de Eduardo Beira, Cristiano Cruz e Ricardo Neder. Vila Nova de Gaia: Inovatec, 2019.

FERREIRA, Aurélio Buarque de Holanda. **Novo Dicionário Aurélio da Língua Portuguesa**. 2. ed. rev. e ampl. Rio de Janeiro: Editora Nova Fronteira, 1986.

FICO, Carlos. **O Grande Irmão**: da Operação Brother Sam aos Anos de Chumbo: o Governo dos Estados Unidos e a Ditadura Militar Brasileira, Editora Civilização Brasileira, 2008.

FIORI, José Luís (org.). **Estados Unidos e a América Latina**: A Construção da Hegemonia. Petrópolis: Vozes, 2007.

FOLHA DE S. PAULO. **É preciso acabar com o modelo digital baseado nos dados pessoais, diz professora**. Disponível em: <https://www1.folha.uol.com.br/tec/2021/01/e-preciso-acabar-com-o-modelo-digital-baseado-nos-dados-pessoais-diz-professora.shtml>. Acesso em: 20 ago. 2023.

FOLHA DE S. PAULO. **Equifax pagará até 700 milhões em acordo sobre violação de dados nos EUA**. Disponível em:

<https://www1.folha.uol.com.br/mercado/2019/07/equifax-pagara-ate-us-700-milhoes-em-acordo-sobre-violacao-de-dados-nos-eua.shtml#:~:text=A%20Equifax%20foi%20multada%20em,os%20armazenado%20n os%20Estados%20Unidos>. Acesso em: 21 ago. 2023.

FONSECA, Ricardo Marcelo. **Introdução Teórica à História do Direito**. Curitiba: Juruá, 2010.

FONSECA, Ricardo Marcelo. Tradições, traduções, traições: diálogos entre culturas jurídicas. **Revista do Instituto Brasileiro de História do Direito – IBHD**, n. 1, v. 1 jul/dez. 2020, p. 4.

FOUCAULT, Michel. **Vigiar e Punir: nascimento da prisão**. Tradução de Raquel Ramallete. 38. ed. Petrópolis: Vozes, 2008.

G1. **Na mídia, pode-se consultar o seguinte: Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades**. Publicado em 20 mar. 2018. 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: 21 ago. 2023.

G1. **Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber**. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml>. Acesso em: 21 ago. 2023.

GAGNON, Jean-Paul. **2,234 Descriptions of Democracy: An Update to Democracy's Ontological Pluralism**. *Democratic Theory*, v. 5, n. 1, p. 92-113, 2018

GASPARI, Elio. **A Ditadura Envergonhada**. Editora Companhia das Letras, 2002.

GATTI, Vanessa Andreza. **Uma Nação Sob o Olhar de Washington: os Estados Unidos e o golpe de 1973 no Chile**. São Paulo: Unesp, 2015.

GOV.BR. Ministério da Saúde. **Amianto: a exposição ao amianto está relacionada à ocorrência de diversas doenças, sobretudo mesotelioma**. Disponível em: <https://www.gov.br/inca/pt-br/assuntos/causas-e-prevencao-do-cancer/exposicao-no-trabalho-e-no-ambiente/amianto>. Acesso em: 15 set. 2023.

GOV.BR. **Regulamento de Transferências Internacionais de Dados Pessoais e do modelo de Cláusulas-Padrão Contratuais**. Disponível em:

<https://www.gov.br/participamaisbrasil/regulamento-de-transferencias-internacionais-de-dados-pessoais-e-do-modelo-de-clausulas-padrao-contratuais#:~:text=A%20ANPD%20poder%C3%A1%20reconhecer%2C%20median te,na%20LG%20PD%20e%20neste%20Regulamento>. Acesso em: 19 jul. 2024.

GOV.BR. **Diário Oficial da União**. Despacho Decisório nº 20/2024/PR/ANPD. Processo nº 00261.004509/2024-36. Interessado: META PLATFORMS INC - FACEBOOK SERVIÇOS ONLINE DO BRASIL. Disponível em: <https://www.in.gov.br/en/web/dou/-/despacho-decisorio-n-20/2024/pr/anpd-569297245>. Acesso em: 10 jul. 2024.

GOV.BR. **Resolução CD/ANPD Nº 19, de 23 de agosto de 2024**. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396>. Acesso em 09 set. 2024.

GOV.BR. Diário Oficial da União. **Despacho Decisório nº 20/2024/PR/ANPD**. Processo nº 00261.004509/2024-36. Interessado: META PLATFORMS INC - FACEBOOK SERVIÇOS ONLINE DO BRASIL. Disponível em: <https://www.in.gov.br/en/web/dou/-/despacho-decisorio-n-20/2024/pr/anpd-569297245>. Acesso em: 10 jul. 2024.

GREEN, James N. **Apesar de Vocês: a Oposição à Ditadura Militar de 1964 a 1985** Companhia das Letras, 2009.

GREENWALD, Glenn. **Sem lugar para se esconder**. Rio de Janeiro: Sextante, 2014.

GRUPO DE ESTUDOS DE DIREITO AUTORAL E INDUSTRIAL. Faculdade de Direito da Universidade Federal do Paraná. **IV Seminário sobre Proteção de Dados Pessoais. Webinar: 5 anos de LGPD**. Disponível em: <https://www.gedai.com.br/iv-seminario-sobre-protecao-de-dados-pessoais-webinar-5-anos-de-lgpd/>. Acesso em: 08 ago. 2023.

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

HOUAISS, Antônio. **Dicionário Houaiss de Sinônimos e Antônimos da Língua Portuguesa**. Rio de Janeiro: Objetiva, 2003.

INTERSOFT CONSULTING. **General Data Protection Regulation - GDPR**. Disponível em: <https://RGPD-info.eu/>. Acesso em: 04 ago. 2023.

IRAMINA, Aline. "RGPD V. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de

Proteção de Dados da União Europeia. **Revista de Direito, Estado e Telecomunicações**, v. 12, n. 2, p. 91-117, out. 2020.

JACOB NETO, Elias. Vigilância ou surveillance? Proposta para começar a compreender corretamente este fenômeno. *In*: ROVER, Aires José; CELLA, José Renato Gaziero; AYUDA, Fernando Galindo (Orgs.). **Direito e Novas Tecnologias**. Florianópolis: CONPEDI, 2014.

JUSBRASIL. **Os efeitos do vazamento de dados das Redes da Sony na legislação brasileira**. Disponível em: <https://www.jusbrasil.com.br/noticias/os-efeitos-do-vazamento-de-dados-das-redes-da-sony-na-legislacao-brasileira/2664002>. Também: https://www.bbc.com/portuguese/noticias/2011/04/110427_sony_hacker_bg. Acesso em: 21 ago. 2023.

KAISER, Brittany. Targeted: ***My inside story of Cambridge Analytica and how Trump, Brexit and Facebook broke democracy***. Nova Iorque: Harper, 2019.

KELSEN, Hans. **Teoria Pura do Direito**. 8. ed. São Paulo: Editora WMF Martins Fontes, 2009.

KURZWEIL, Ray. **A Era das Máquinas Espirituais**. São Paulo: Aleph, 2007.

LANDER, Edgardo (Org.). **A colonialidade do saber: eurocentrismo e ciências sociais: perspectivas latino-americanas**. Buenos Aires: CLACSO, 2005.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2011.

LIMA, Abili Lázaro Castro de. **Globalização econômica, política e direito: análise das mazelas no plano político-jurídico**. Porto Alegre: Sérgio Fabris, 2002.

MACHADO, Débora Franco. A colonização dos dados como produto das operações das mídias sociais no sul global. *In*: **Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal**. Autonomia Literária, 2021. p. 51-66.

MAGRANI, Eduardo (Ed.). **Digital rights: Latin America and the Caribbean**. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, 2017.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **Comentários ao GDPR**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019; MARTINS, Antônio Eduardo Senna. Comparando a LGPD com a GDPR: abordagens à proteção de dados pessoais. Jusbrasil, 2023.

MARTINS, Antônio Eduardo Senna. Comparando a LGPD com a GDPR: Abordagens à Proteção de Dados Pessoais. **JusBrasil**. Disponível em:

<https://www.jusbrasil.com.br/artigos/comparando-a-lgpd-com-a-gdpr-abordagens-a-protecao-de-dados-pessoais/1971798734>. Acesso em: 10 jul. 2024.

MATTEUCCI, Nicola. Organización del poder y libertad. **Historia del constitucionalismo moderno**, Madrid, Trotta, 1998

MENDES, Aquilas Nogueira. O Consenso de Washington, vulnerabilidade externa e a superexploração do trabalho na América Latina: uma análise à luz da Teoria Marxista da Dependência. **De Raíz Diversa: Revista Especializada em Estudios Latino Americanos**, v. 8, n. 15, 2021.

MENDES, João. A Segurança na Proteção de Dados: Entre o RGPD Europeu e a LGPD Brasileira. **Revista do CEJUR/TJSC: Prestação Jurisdicional**, v. 4, n. 8, p. 346-365, 2019.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2013.

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares. STF reconhece direito fundamental à proteção de dados: comentários sobre o referendo da medida cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393, **Revista de Direito do Consumidor**, v. 130/2020, p. 471-478, Jul - Ago/2020.

MENDES, Laura Schertel; GICO JUNIOR, Ivo Teixeira. Autodeterminação informativa e proteção de dados pessoais: fundamentos, experiências internacionais e perspectivas para o Brasil. **Revista de Direito Administrativo**, v. 272, p. 121-150, 2016.

MESQUITA, Mário. **A União Europeia como potência global? As alterações do Tratado de Lisboa na política externa e de defesa**. Revista Brasileira de Política Internacional, v. 54, n. 1, p. 178-196, 2011.

MIGNOLO, Walter D. **The darker side of western modernity**: global futures, decolonial options. Durham: Duke University Press, 2011.

MIGNOLO, Walter D. Desobediência epistêmica: a opção decolonial e o significado de identidade no pensamento crítico latino-americano contemporâneo. In: CANDAU, Vera M. (org.). **Globalização e educação**: desafios para políticas e práticas pedagógicas. São Paulo: Cortez, 2015.

MORAIS, José Luis Bolzan de; MENEZES NETO, Elias Jacob de. A insuficiência do marco civil da internet na proteção das comunicações privadas armazenadas e do fluxo de dados a partir do paradigma da *surveillance*. In: LEITE, George Salomão;

LEMOS, Ronaldo (coords). **Marco Civil da Internet**. São Paulo: Atlas, 2014, p. 417-439.

MOREIRA, Braitner. Netsshoes deverá procurar 2 milhões de clientes afetados por vazamento, diz MP. **G1-DF**. Publicado em 26 jan. 2018. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/mp-pede-que-netsshoes-tome-providencia-apos-vazamento-de-2-milhoes-de-contas.ghtml>. Acesso em: 20 ago. 2023.

MÜLLER, Friedrich. **Quem é o povo?: a questão fundamental da democracia**. 7 ed. rev. e atual. São Paulo: Editora Revista dos Tribunais, 2013.

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE. Disponível em: <https://www.nsa.gov/about/mission-strategy/>. Acesso em: 30 ago. 2023.

NEWMAN, Abraham; POSNER, Elliot. **Putting the EU in its place: policy strategies and the global regulatory context**. *Journal of European Public Policy*, v. 22, n. 9, p. 1316-1335, 2015.

O GLOBO. **Estados Unidos acusam quatro militares chineses por roubo de dados de quase 150 milhões de pessoas**. Publicado em 10 fev. 2020 Disponível em: <https://oglobo.globo.com/mundo/estados-unidos-acusam-quatro-militares-chineses-por-roubo-de-dados-de-quase-150-milhoes-de-pessoas-24240625>. Acesso em: 21 ago. 2023.

ORDEM DOS ADVOGADOS DO BRASIL - OAB NACIONAL. **Três anos de vigência da LGPD: Os principais avanços na proteção de dados no Brasil - Homenagem a Danilo Doneda** – Disponível em: <https://www.ab.org.br/noticia/61194/oab-abre-seminario-sobre-avancos-da-lgpd-com-homenagem-ao-pesquisador-danilo-doneda>. Acesso em: 08 ago. 2023.

ORWELL, George. **1984**. 29. ed. São Paulo: Companhia Editora Nacional, 2005.

PATEMAN, Carole. **Participação e teoria democrática**. Rio de Janeiro: Paz e Terra, 1992.

PAGALLO, Ugo. The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection. **Eur Law J.**, v. 24, n. 6, p. 533-555, 2018.

PAULA, João Antônio de; PEREIRA, Luiz Carlos Bresser. **A macroeconomia da estagnação: crítica da ortodoxia neoliberal e o novo desenvolvimentismo**. 2. ed. São Paulo: Ed. 34, 2020.

PHILARCHIVE.ORG. **Views on Privacy.** a survey. Disponível em: <https://philarchive.org/rephilarchive.org/BROVOP-3>. Acesso em: 20 ago. 2023.

PINHEIRO, Patrícia Peck. Análise comparativa com o regulamento europeu (GDPR). *In*: PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei 13.709/2018 (LGPD)**. Saraiva Jur. 2021.

PODER 360. **Megavazamento global expõe 10 milhões de senhas de e-mails brasileiros.** Disponível em: <https://www.poder360.com.br/tecnologia/megavazamento-global-expoe-10-milhoes-de-senhas-de-e-mails-brasileiros/>. Acesso em: 21 ago. 2023.

QUAN-HAASE, Anabel; WELLMAN, Barry. Distance and Media: a case study of a high tech firm. **Trust and Communities Conference**, July, Bielefeld.

QUIJANO, Aníbal. Colonialidade do poder, eurocentrismo e América Latina. *In*: LANDER, Edgardo (Org.). **A colonialidade do saber: eurocentrismo e ciências sociais: perspectivas latino-americanas**. Buenos Aires: CLACSO, 2005. [Recurso em meio eletrônico].

QUIJANO, Aníbal. **América: el capitalismo y la modernidad nacieron el mismo día.** ILLA (Lima) N° 10, janeiro; Quijano, Aníbal 1992 “Colonialidad y modernidad/racionalidad” em *Perú Indígena* (Lima) v. 13, n. 29.

RAMOS, Alberto Guerreiro. **A redução sociológica: introdução ao estudo da razão sociológica.** Rio de Janeiro: Edições Tempo Brasileiro, 1996.

RECLAME AQUI. **Netshoes.** Disponível em: <https://www.reclameaqui.com.br/empresa/netshoes/>. Acesso em: 20 ago. 2023.

RECLAME AQUI. **Como funcionam os critérios para avaliação das empresas?** Disponível em: <https://www.reclameaqui.com.br/como-funciona/reputacao/>. Acesso em: 20 ago.2023.

RÉ, Henrique Antonio. A revogação do Bill Aberdeen e a Lei do Ventre Livre: um acordo antiescravista internacional 1864-1872. **Rev. Hist.**. São Paulo, nº 178, 2019.

RIBEIRO, Darcy. **O povo brasileiro: a formação e o sentido do Brasil.** 3. ed. São Paulo: Global, 2015.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje.** Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RODOTÀ, Stefano. Democracia y protección de datos, **Cuadernos de Derecho Público**, n. 19-20, mayo-diciembre, 2003.

SADER, Emir. **A vingança da história**: o neoliberalismo e os seus destinos. São Paulo: Boitempo, 2013.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 10. ed. rev. atual. e ampl.; 3ª tiragem. Porto Alegre: Livraria do Advogado Editora, 2011.

SARLET, Ingo Wolfgang; SAAVEDRA, Giovani Agostini. Fundamentos jusfilosóficos e âmbito de proteção do direito fundamental à proteção de dados pessoais, **RDP**, Brasília, v. 17, n. 93, 33-57, maio/jun. 2020.

SARLET, Ingo Wolfgang. **Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988**: contributo para a construção de uma dogmática constitucionalmente adequada. Direitos Fundamentais e Justiça [Recurso em meio eletrônico]. Belo Horizonte, v.14, n.42, jan./jun. 2020.

SARLET, Ingo Wolfgang. A EC 115/22 e a proteção de dados pessoais como Direito Fundamental I. **Conjur**, 11 de março de 2022.

SCHITTINO, Renata. **Chile**: o Golpe e o Impacto no Cone Sul. Rio de Janeiro: Mauad X, 2013.

SGARBI, Adrian. **Curso de Teoria do Direito**. 2. ed. Rio de Janeiro: Lumen Juris, 2021, p. 61.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 34. ed. rev. e atual. São Paulo: Malheiros Editores, 2011.

SILVA, Rodrigo Frogeri da; ALEGÁRIO, Cibele Cristina. Os Impactos da Lei Geral de Proteção de Dados (LGPD) no Cenário Digital. **Revista de Direito, Estado e Telecomunicações**, v. 12, n. 2, p. 27-50, out. 2020.

SOUZA, Carlos Affonso Pereira de. O progresso tecnológico e a tutela jurídica da privacidade. Rio de Janeiro: PUC-Rio, **Revista de Direito, Estado e Sociedade**, v. 9, n. 16, p. 6-39, jan-jul, 2000.

SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (Coords.). **Lei Geral de Proteção de Dados**. Caderno Especial, novembro, Thomson Reuters - Revista dos Tribunais, 2019.

STOLLEIS, Michael. **Escrever História do Direito**: reconstrução, narrativa ou ficção? São Paulo: Editora Contracorrente, 2020, p. 60-61.

THALER, Richard H.; SUNSTEIN, Cass R. **Nudge: como tomar melhores decisões sobre saúde, dinheiro e felicidade**. Tradução de Regina Lyra. 2. ed. Rio de Janeiro: Objetiva, 2019.

SUPREMO TRIBUNAL FEDERAL. **Especial Meio Ambiente: STF proíbe extração e venda de amianto crisotila**. Disponível em: <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=509089&ori=1>. Acesso em: 15 set. 2023.

SUPREMO TRIBUNAL FEDERAL. **Recursos públicos não podem ser utilizados para promover comemorações do golpe de 1964, decide STF**. Publicado em 24 set. 2024. Disponível em: <https://noticias.stf.jus.br/postsnoticias/recursos-publicos-nao-podem-ser-utilizados-para-promover-comemoracoes-do-golpe-de-1964-decide-stf/>. Acesso em: 29 set. 2024.

TEIXEIRA, Tarcísio. **Direito digital e processo eletrônico**. 5. ed. São Paulo: Saraiva Educação, 2020.

TENABLE. **Relatório do cenário de ameaças de 2022 da Tenable**. Disponível em: <https://pt-br.tenable.com/cyber-exposure/tenable-2022-threat-landscape-report>. Acesso em: 21 ago. 2023.

TECNOBLOG. **Megavazamento de 223 milhões de CPFs: um ano se passou e ainda há perguntas sem resposta**. <https://tecnoblog.net/especiais/megavazamento-de-223-milhoes-de-cpfs-um-ano-se-passou-e-ainda-ha-perguntas-sem-resposta/>. Acesso em: 21 ago. 2023.

VÉLIZ, Carissa. University of Oxford. Institute for Ethics in AI. University of Oxford. Disponível em: <https://www.carissaveliz.com/>. Acesso em: 15 set. 2023.

VÉLIZ, Carissa. **Privacidade é poder: por que razão e como devemos recuperar o controle dos nossos dados**. 2022. Tradução Samuel Oliveira. Contracorrente, 2021.

VERKERK, Maarten J.; HOOGLAND, Jan; VAN DER STOEP, Jan; DE VRIES, Marc J. **Filosofia da Tecnologia: uma introdução**. Tradução de Valter Martins. Viçosa: Ultimato, 2018.

VERIZON. Disponível em: <http://www.verizon.com/about/our-company/who-we-are>. Acesso em: 01 fev. 2017.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. Porto Alegre: Fabris, 2007.

VILLA, Marco Antonio. **A história das constituições brasileiras**: 200 anos de luta contra o arbítrio. São Paulo: Leya, 2011.

VILLA, Marco Antonio. **Ditadura à brasileira: 1964-1985: a democracia golpeada à esquerda e à direita**. São Paulo: Leya, 2014.

VIOLA, Mario. **A proteção de dados pessoais no Brasil e na União Europeia: uma análise comparativa**. In: MENDES, Laura Schertel; VIOLA, Mario; OLIVEIRA, Gustavo (Orgs.). *Proteção de dados: desafios e tendências*. São Paulo: Thomson Reuters Brasil, 2019.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2019.

WALLERSTEIN, Immanuel. **Capitalismo histórico e civilização capitalista**. Rio de Janeiro: Ed. Contraponto, 2001.

WALSH, Catherine. **La insubordinación fundante: América Ladina y el giro decolonial**. Quito: Universidad Andina Simón Bolívar, Ediciones Abya-Yala, 2012

WARREN, Samuel D. and BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, Dec. 15, 1890, p. 193-220.

ZANATTA, Rafael Augusto Ferreira; ABRAMOVAY, Ricardo. Dados pessoais abertos: pilares dos novos negócios. **RDU**, Porto Alegre, Volume 16, n. 90, 2019, 155-178, nov./dez. 2019.

ZANON, João Carlos. **Direito à proteção dos dados pessoais**. São Paulo: Revista dos Tribunais, 2013.