UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

REGINALDO FELIX NASCIMENTO

EFETIVIDADE DO DIREITO À PRIVACIDADE NA TRANSFERÊNCIA INTERNACIONAL DE DADOS SOB A LEI GERAL DE PROTEÇÃO DE DADOS DO BRASIL

SÃO CRISTOVÃO
2024

REGINALDO FELIX NASCIMENTO

EFETIVIDADE DO DIREITO À PRIVACIDADE NA TRANSFERÊNCIA INTERNACIONAL DE DADOS SOB A LEI GERAL DE PROTEÇÃO DE DADOS DO BRASIL

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal de Sergipe – UFS, como requisito à obtenção do título de Mestre em Direito.

Orientador: Prof. Dr. Lucas Gonçalves da Silva

SÃO CRISTOVÃO

2024

REGINALDO FELIX NASCIMENTO

EFETIVIDADE DO DIREITO À PRIVACIDADE NA TRANSFERÊNCIA INTERNACIONAL DE DADOS SOB A LEI GERAL DE PROTEÇÃO DE DADOS DO BRASIL

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal de Sergipe, como último requisito para a obtenção do Título de Mestre em Direito. Esta dissertação foi julgada e aprovada pela comissão abaixo assinada em 15 de Janeiro de 2025.

São Cristóvão, Sergipe, Brasil

_____

Prof. Dr. Lucas Gonçalves da Silva – Orientador
Universidade Federal de Sergipe – UFS

_____

Dr. Henrique Ribeiro Cardoso – Membro Interno
Universidade Federal de Sergipe – UFS

_____

Dr. Liton Lanes Pilau Sobrinho – Membro Externo
Universidade de Passo Fundo – UPF

Dedico este trabalho à minha mãe e à minha avó, que sempre acreditaram em mim e me apoiaram incondicionalmente, mesmo diante das minhas inconsistências.

[…] Eu amo o Longe e a Miragem,
Amo os abismos, as torrentes, os desertos...
Ide! Tendes estradas,
Tendes jardins, tendes canteiros,
Tendes pátria, tendes tetos,
E tendes regras, e tratados, e filósofos, e sábios...
Eu tenho a minha Loucura!
Levanto-a, como um facho, a arder na noite escura,
E sinto espuma, e sangue, e cânticos nos lábios...
Deus e o Diabo é que guiam, mais ninguém!
Todos tiveram pai, todos tiveram mãe;
Mas eu, que nunca principio nem acabo,
Nasci do amor que há entre Deus e o Diabo.
Ah, que ninguém me dê piedosas intenções,
Ninguém me peça definições!
Ninguém me diga: "vem por aqui"!
A minha vida é um vendaval que se soltou,
É uma onda que se alevantou,
É um átomo a mais que se animou… […]

Cântico Negro – José Régio

AGRADECIMENTOS

Gostaria de dedicar este espaço de gratidão a todos aqueles que, de maneira única e essencial, foram responsáveis por tornar possível esta jornada.

Primeiramente, Grato a Deus, em quem duvidei por muito tempo, mas que me levou a crer em algo maior, pelas coisas extraordinárias e inexplicáveis que ocorreram em minha vida.

Minha gratidão ao Professor Dr. Lucas, cuja motivação e orientação foram fundamentais para minha jornada. Seu tratamento humanizado e suas palavras sempre me incentivaram a seguir em frente, especialmente nos momentos mais desafiadores. A forma como me guiou, sempre com paciência e sensibilidade, teve um impacto profundo, e sou imensamente grato por sua presença, que foi muito mais do que uma simples orientação acadêmica.

Não posso deixar de agradecer aos meus professores, Dr. Henrique, Dra. Clara Angélica e Dr. Jadson, pela sabedoria, generosidade e por se tornarem uma inspiração.

À coordenação do programa de pós-graduação em Direito, especialmente à Dra. Clara Angélica, minha profunda gratidão pela liderança exemplar que transformou esse processo em algo fluído e tranquilo. A Nayara, servidora da coordenação, também merece meu agradecimento por sua disposição e apoio em todos os momentos.

Ao fomento da CAPES, que, por meio da concessão da bolsa, me proporcionou a liberdade para dedicar-me integralmente à pesquisa, sem as limitações financeiras que muitas vezes impedem o progresso acadêmico. Este apoio foi fundamental para a realização deste trabalho e sou eternamente grato.

Aos ilustres professores Dr. Umberto Celli Junior e Dr. Caio Gracco, agradeço profundamente pelos ensinamentos que enriqueceram minha formação intelectual.

Meu sincero agradecimento ao Maestro João Flávio, meu professor de Violino, cujo ensinamento foi mais do que técnico: foi uma lição de vida. Sua orientação, paciência e sabedoria foram fundamentais para que eu chegasse mais longe, não só na música, mas também na vida.

Aos meus colegas da 1ª Vara Cível de Aracaju (SE), Breno, Isabela, Paula, Carol, Helô e Nelma, minha gratidão por me acolherem com tanto carinho e por

proporcionarem uma experiência que foi, sem dúvida, enriquecedora e transformadora. Aprendi muito com cada um de vocês.

Ao meu querido chefe Dr. Anderson Rochão, minha profunda admiração. Sua visão, inteligência e, acima de tudo, sua confiança, foram essenciais para meu crescimento. Agradeço por ser um mentor e exemplo de integridade e humanidade.

Aos meus colegas de trabalho, Ubirajara, Estefanie e Dagmar, meu mais sincero obrigado. O trabalho ao lado de pessoas tão incríveis e dedicadas tornou os dias mais leves e significativos. Sou grato por cada momento compartilhado.

Meus tios – Regi da DESO, Zé da Farmácia, Raimundo da ARV, Julhinho da Cerâmica e Nicinho da Cerâmica – agradeço pela imensa inspiração que são. Cada um de vocês, com sua trajetória de dedicação e perseverança, tem sido pilar fundamental em minha vida, me mostrando que, com esforço, não há limites para as conquistas.

Gostaria de destacar, de forma especial, minha tia Reninha e meu tio Regi, que me ofereceram um lar e, também, carinho. Sem o apoio de vocês, a conclusão do curso de Direito não teria sido possível. Sou eternamente grato por tudo o que fizeram por mim.

À minha avó (Dona Valdete) e minha mãe (Dona Niete), sem vocês este trabalho não teria sido possível. A fé inabalável e o amor constante foram a âncora que me manteve firme nos momentos de dúvida e incerteza. Agradeço por serem o alicerce sobre o qual construí minha jornada.

À minha irmã Bel, pelo apoio constante e por sempre estar ao meu lado. Sua presença foi fundamental para que eu seguisse em frente, oferecendo motivação nos momentos difíceis. Sou muito grato por tudo o que você representa em minha vida.

Aos meus primos Helder e Helis, pelos quais nutro um carinho especial, minha imensa gratidão. A existência de vocês em minha vida sempre trouxe alegria e apoio, e sou muito grato por compartilhar tantos momentos ao lado de pessoas tão queridas.

A Vitor, cuja paciência e apoio foram fundamentais para o êxito deste trabalho. Sua capacidade de me motivar e de acreditar em mim nos momentos mais desafiadores fez toda a diferença. Sou profundamente grato por sua presença constante e pelo suporte em cada passo dessa caminhada.

À minha querida colega de orientação, Camilla, minha gratidão profunda por sua inteligência brilhante e pela parceria tão especial durante todo este processo. A cada dilema, sua colaboração foi essencial, e sou imensamente grato por ter tido a oportunidade de trabalhar ao seu lado. Sua intelectualidade é um verdadeiro modelo, mas, acima de tudo, é sua generosidade e apoio que tornaram essa jornada ainda mais significativa.

Ao grupo “Autoridades” – Rennan, Karla, Hayalla, Camilla e Nicole – vocês foram essenciais para minha saúde mental durante os períodos mais difíceis do mestrado. As conversas e risadas compartilhadas aliviaram o estresse e me proporcionaram uma leveza necessária para seguir em frente. Meu muito obrigado, de coração.

Ao Conselho JEDI, Silas, Ithala e Yago, agradeço pela resistência e resiliência que me ajudaram a cultivar. Com humor e perspicácia, vocês me ensinaram a enfrentar os obstáculos com coragem e serenidade. Sou grato pela amizade e pela força que emanam.

Por fim, a todas as pessoas que de alguma forma contribuíram para a realização deste sonho, meu muito obrigado. Cada palavra de incentivo, cada gesto de apoio, cada presença ao meu lado foi essencial para que chegasse até aqui. Este trabalho reflete a colaboração de todos, e sou imensamente grato por cada contribuição, grande ou pequena, que tornou esta jornada possível.

RESUMO

A globalização, aliada às tecnologias de informação e comunicação, transferiu as práticas econômicas globais para o ambiente virtual. Isso demandou uma catalogação constante de aspectos consideráveis da vida, como dados genéticos, biométricos, raciais, de orientação sexual, de gênero, fiscais, de crédito, entre outros, que levaram a uma economia invasiva, questionada juridicamente acerca da sua intervenção na liberdade dos cidadãos. Dado o contexto apresentado, este trabalho aborda a seguinte problemática: considerando a transferência internacional de dados como um vetor da economia contemporânea, há efetividade do direito à privacidade na regulação dos fluxos internacionais de dados pessoais? Partindo da análise da Lei Geral de Proteção de Dados Pessoais (LGPD) e do Regulamento de Transferência Internacional de Dados do Brasil (Resolução n. 19/2024 da ANPD), a dissertação tem como objetivo geral investigar a efetividade do direito à privacidade na transferência internacional de dados pessoais, com os seguintes objetivos específicos: (I) compreender os pressupostos e a evolução histórica do Direito à Privacidade e da Proteção de Dados Pessoais; (II) fazer uma análise comparativa dos marcos regulatórios nacionais, estrangeiros e internacionais de proteção de dados pessoais e do direito à privacidade; (III) diagnosticar as bases legais da transferência internacional de dados pessoais no Brasil; (IV) compreender a efetividade do direito à privacidade dos titulares de dados do Brasil na Transferência Internacional de Dados. O trabalho detém as seguintes hipóteses: I) o estudo dos postulados fundamentais do Direito à Proteção de Dados Pessoais proporcionará *insights* valiosos para a regulação das transferências internacionais de dados, revelando aspectos cruciais sobre a efetividade do Direito à Privacidade; (II) a compreensão dos aspectos jurisdicionais envolvidos, bem como dos padrões jurídicos do GDPR e dos padrões de dados da América Latina, permitirá identificar dilemas de efetividade do direito à privacidade; (III) A análise da Lei Geral de Proteção de Dados Pessoais do Brasil exporá se a abordagem regulatória nacional é suficiente ou não para proteger a transferência internacional de dados pessoais; (IV) a investigação das práticas regulatórias nacionais, estrangeiras e internacionais e de concepções aliadas auxiliarão na determinação de uma maior efetividade para o Direito à Privacidade no Brasil.

Palavras-chave: Globalização; Proteção de dados; Direito à Privacidade; LGPD; Transferência Internacional de Dados; Regulamento de Transferência Internacional de Dados; Jurisdição e Internet; Proteção de Dados e Direito Comparado.

ABSTRACT

Globalization, combined with advancements in information and communication technologies, has shifted global economic practices into the virtual realm. This shift has necessitated the constant cataloging of significant aspects of life, such as genetic, biometric, racial, sexual orientation, gender, tax, and credit data, among others. As a result, an invasive economy has emerged, raising legal concerns regarding its interference with individual freedoms. In light of this context, this work addresses the following question: Considering the international transfer of data as a cornerstone of the contemporary economy, is the right to privacy effective in regulating the cross-border flow of personal data? By analyzing Brazil's General Data Protection Law (LGPD) and the Brazilian International Data Transfer Regulation (ANPD Resolution No. 19/2024), this dissertation aims to investigate the effectiveness of the right to privacy in the context of international personal data transfers. The first specific objective is to examine the historical evolution and foundational principles of the Right to Privacy and Personal Data Protection. The second specific objective is to conduct a comparative analysis of national, foreign, and international regulatory frameworks for personal data protection and the right to privacy. The third specific objective is to identify the legal bases for international personal data transfers in Brazil.The fourth specific objective is to assess the effectiveness of the right to privacy for data subjects in Brazil within the context of international data transfers.The first hypothesis is that an analysis of the fundamental principles of the Right to Personal Data Protection will provide valuable insights into the regulation of international data transfers, shedding light on the effectiveness of the Right to Privacy. The second hypothesis is that an understanding of jurisdictional aspects, as well as the legal standards of the GDPR and data protection frameworks in Latin America, will help identify challenges to the effectiveness of the right to privacy. The third hypothesis is that an examination of Brazil's General Data Protection Law (LGPD) will reveal whether the national regulatory framework is sufficient to safeguard international personal data transfers. The fourth hypothesis is that an investigation of national, foreign, and international regulatory practices, along with related concepts, will contribute to determining greater effectiveness for the Right to Privacy in Brazil.

Keywords: Globalization; Data protection; Right to Privacy; LGPD (General Data Protection Law); International Data Transfer; International Data Transfer Regulation; Jurisdiction and the Internet; Data Protection and Comparative Law.

LISTA DE SIGLAS E ABREVIATURAS

ADI	Ação Direta de Inconstitucionalidade
AEPD	Agência Espanhola de Proteção de Dados
ANPD	Autoridade Nacional de Proteção de Dados
APEC	Asia-Pacific Economic Cooperation
BCR	Binding Corporate Rules
EC	Emenda Constitucional
EUA	Estados Unidos
GATS	Acordo Geral sobre Comércio de Serviços
GDPR	General Data Protection Regulation
LGBT+	Lésbicas, Gays, Bissexuais, Transexuais entre outros
LGPD	Lei Geral de Proteção de Dados Pessoais
NCG	Normas Corporativas Globais
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OEA	Organização dos Estados Americanos
ONU	Organização da Nações Unidas
SIC	Superintendência de Indústria e Comércio da Colômbia
STF	Supremo Tribunal Federal
T-MEC	Acordo Estados Unidos-México-Canadá
TEDH	Tribunal Europeu de Direitos Humanos
TICs	Tecnologias de Informação e Comunicação
TID	Transferência Internacional de Dados
TJUE	Tribunal de Justiça da União Europeia
TO	Tocantins
URCDP	Unidade Reguladora e de Controle de Dados Pessoais do Uruguai
WWW	World Wide Web

SUMÁRIO

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados (Lei n. 13.709/2018) estabeleceu diversas regras para a proteção e o tratamento de dados no Brasil. No seu texto, destaca-se o Capítulo V, denominado “Da Transferência Internacional de Dados Pessoais’’. Esse capítulo abrange os artigos 33 a 36, que estabelecem as bases legais que sustentam a transferência internacional de dados no Brasil. No dia 23 de agosto de 2024, a Autoridade Nacional de Dados (ANPD) publicou a resolução CD/ANPD Nº 19, que instituiu o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais do Brasil.

Diante disso, percebe-se uma preocupação do legislador e da Autoridade Nacional de Proteção de Dados (ANPD) em proteger a transferência internacional de dados pessoais, o que justifica a elaboração do presente trabalho. Ademais, segundo as informações levantadas por Suda (2017), entre 2005 e 2014, as transferências internacionais de dados aumentaram 45 vezes em escala global. Em 2015, conforme dados expostos por Bräutigam (2016), 76 *exabytes* de dados foram movimentados por meio digital. Além disso, Alhababi (2024) assevera que, no ano de 2014, os fluxos internacionais de dados contribuíram para a geração de US$ 2,8 trilhões para o PIB mundial.

O tema em questão se insere nas grandes áreas de Direito Constitucional e Direito Digital, com uma sub-área focada na efetividade dos Direitos Fundamentais diante da globalização e das novas tecnologias. Em um contexto em que as fronteiras geográficas se tornam cada vez mais tênues no campo digital, questões relacionadas à privacidade e à proteção de dados pessoais ganham relevância. A globalização tem ampliado a troca de informações em nível internacional, enquanto as novas tecnologias geram impactos sobre como garantir que os direitos fundamentais, especialmente o direito à privacidade, sejam respeitados e protegidos, independentemente de onde os dados estejam sendo coletados ou processados. A efetividade desses direitos, portanto, se torna um ponto central para assegurar que as inovações tecnológicas não comprometem as garantias constitucionais dos indivíduos.

Quanto às contribuições para a linha de pesquisa “processo de constitucionalização dos direitos e cidadania: aspectos teóricos e metodológicos’’, ao investigar o direito à privacidade como um direito fundamental tutelado pela

Constituição, examinando como a Lei de Proteção de Dados efetiva tal direito na transferência internacional de dados pessoais, a dissertação visa compreender a constitucionalização dos direitos no Brasil, questionando se as leis infraconstitucionais e os regulamentos satisfazem os direitos fundamentais. Nesse caso, o alinhamento com a linha de pesquisa do Programa de Pós-graduação em Direito da Universidade Federal de Sergipe (PRODIR/UFS) reside, também, na dedicação de tópico exclusivo para tratar da constitucionalização do direito à proteção de dados pessoais [subitem 2.2 – O Direito à Proteção de Dados Pessoais e a Constitucionalização do Direito no Brasil] e na análise da conformidade da regulação da transferência internacional de dados com o Direito Fundamental à Privacidade.

À vista disso, a efetividade do direito à privacidade na transferência internacional de dados está conectada com a cidadania, pois a proteção de dados é intimamente ligada à qualidade e segurança do exercício da cidadania na internet. Ademais, percebe-se o desenvolvimento de novos objetos jurídicos, que exploram os limites e a aplicabilidade do direito à privacidade, permitindo reinterpretar a privacidade no marco da constitucionalização dos direitos. Ao questionar os desafios de implementação da Lei Geral de Proteção de Dados e a própria efetividade do direito à privacidade, esta dissertação avança no debate metodológico sobre a aplicação das normas de privacidade. Tais pontos contemplam as vertentes teóricas e metodológicas da linha de pesquisa, oferecendo perspectivas diversificadas acerca da constitucionalização do direito à privacidade no âmbito do Direito Interno, considerando a globalização e as Tecnologias de Informação e Comunicação (TICs).

A dissertação aborda a seguinte questão central: considerando a regulação da transferência internacional de dados, em que medida o direito à privacidade é efetivamente protegido nos fluxos internacionais de dados pessoais?

Quanto ao objetivo geral, este trabalho visa perscrutar a efetividade do Direito Fundamental à Privacidade na Transferência Internacional de Dados, levando em consideração a Lei Geral de Proteção de Dados do Brasil e o Regulamento de Transferência Internacional de Dados do Brasil (Resolução n. 19/2024 da ANPD). Além disso, objetivos específicos foram empregados no sentido de: (I) compreender os pressupostos e a evolução histórica do Direito à Privacidade e da Proteção de Dados Pessoais; (II) fazer uma análise comparativa dos marcos regulatórios

nacionais, estrangeiros e internacionais de proteção de dados pessoais e do direito à privacidade; (III) diagnosticar as bases legais da transferência internacional de dados pessoais no Brasil; (IV) compreender a efetividade do direito à privacidade dos titulares de dados do Brasil na Transferência Internacional de Dados.

A dissertação adere ao método hipotético-dedutivo, cuja pesquisa detém natureza qualitativa, caracterizada pela investigação documental e bibliográfica acerca da efetividade da tutela jurídica da proteção das transferências internacionais de dados e assuntos correlatos ao tema. Além das abordagens temáticas histórico-evolutiva, comparativa e dogmática, a dissertação conta com*:* revisão bibliográfica, a partir de textos buscados nos indexadores/bibliotecas a partir das palavras-chave: “proteção de dados pessoais’’, “privacidade’’ e “transferências internacionais de dados’’; análise documental de legislações estrangeiras, internacionais e nacionais; estudos de caso, com interpretação de casos concretos afins as discussões travadas nesta dissertação.

Um aspecto metodológico fundamental que deve ser destacado é quanto ao objeto deste trabalho. Para torná-lo inteligível, destaca-se que o foco da pesquisa é a privacidade enquanto direito, com relevância predominantemente constitucional, embora também tenha significativa importância no âmbito internacional. Não se pretende, aqui, tratar como objeto central o conflito entre o direito à privacidade e o livre comércio, tampouco oferecer soluções para conciliá-los. O objetivo principal se baseia em duas premissas: o direito à privacidade é constitucionalmente inegociável; e, consequentemente, a transferência internacional de dados deve garantir sua efetividade.

Na continuidade da exposição dos aspectos metodológicos, apresenta-se cada capítulo, com o detalhamento da sua posição metodológica. Nesse sentido, o capítulo 2 teve como objetivo demonstrar a relevância jurídica do Direito à Privacidade enquanto Direito Fundamental, o que implica que, considerando o interesse constitucional, há a imposição de um dever associado à Transferência Internacional de Dados.

Na sequência, o capítulo 3 apresenta três questões centrais para compreender sua posição metodológica. Primeiramente, destaca-se que a transferência internacional de dados enfrenta um problema de natureza eminentemente jurisdicional, justificando a análise desenvolvida no subitem 3.1. Em

segundo lugar, enquanto o capítulo 2 enfatiza a relevância constitucional do Direito à Privacidade, surge a necessidade de explicar por que esse direito também possui relevância internacional, o que fundamenta o subitem 3.2. No fim, o subitem 3.3 aborda dois aspectos regulatórios essenciais para entender a posição do Brasil no cenário global: o primeiro, relacionado à compreensão do padrão europeu, que serve de inspiração para o país; e o segundo, condicionado ao padrão latino-americano, no qual o Brasil está regionalmente inserido.

No capítulo 4, os seguintes pontos merecem destaque: o subitem 4.1 serve para apresentar o caso brasileiro de forma descritiva, sem juízo de valor; o subitem 4.2, busca realizar uma análise crítica dos elementos descritos no subitem anterior, comparando-os com os aspectos envolvidos nos capítulos 2 e 3; e o subitem 4.3, visa propor soluções com base nas situações identificadas na análise feita no subitem 4.2.

Distintamente do que foi apresentado anteriormente, a seguinte parte da introdução tem o objetivo exclusivo de explicar o conteúdo dos capítulos de forma mais robusta e descritiva, sem abordar sua posição metodológica. Assim, o Capítulo 2, intitulado “Fundamentos da Proteção de Dados”, discute o desenvolvimento histórico e jurídico do direito à privacidade, enfatizando sua evolução desde conceitos antigos até a sua incorporação nas leis modernas de proteção de dados. Ele destaca a transformação do direito à privacidade de um direito ligado à propriedade e ao isolamento individual para um direito mais abrangente, que se preocupa com a dignidade humana e a autonomia individual.

O capítulo expõe como o direito à privacidade foi inicialmente concebido para proteger indivíduos de intrusões indevidas em suas vidas pessoais, especialmente com o advento da imprensa e outras formas de mídia. À medida que a sociedade se tornou mais digitalizada, o capítulo explora como esse direito teve que se adaptar para abordar as complexidades da era da informação, incluindo questões sobre o controle de dados pessoais e o impacto das tecnologias de vigilância.

Ao longo do texto, são discutidas várias perspectivas jurídicas e teóricas sobre o direito à privacidade, oferecendo um panorama de como diferentes sistemas legais e culturas interpretam e aplicam esses princípios. Isso inclui a discussão sobre a dualidade entre visões reducionistas, que vinculam privacidade estritamente à

proteção da propriedade, e visões não reducionistas, que veem a privacidade como um direito intrinsecamente ligado a outros direitos fundamentais.

O Capítulo 3 trata da transferência internacional de dados pessoais, destacando os dilemas jurídicos que envolvem esse tema no contexto mundial. Desde o início da proteção de dados na Alemanha, em 1970, quando ainda não havia regras específicas para transferências internacionais, países europeus rapidamente adotaram medidas restritivas. O objetivo era impedir que dados fossem enviados para locais sem regulamentações adequadas, especialmente à medida que essas transferências se tornaram mais comuns com a expansão da globalização.

O capítulo também reflete sobre como as tensões entre soberania nacional e jurisdição se agravaram com a intensificação dos fluxos internacionais de dados, especialmente após episódios marcantes, como as revelações de Edward Snowden em 2013. Tais acontecimentos impulsionaram discussões sobre vigilância e proteção de dados no âmbito internacional. Nesse cenário, o princípio da territorialidade, tradicionalmente utilizado para delimitar jurisdições, tem sido substituído por abordagens mais flexíveis, como o princípio da personalidade, que aplica as leis com base na nacionalidade do titular dos dados. Essas mudanças evidenciam que os métodos jurídicos tradicionais já não são suficientes para lidar com a interconexão global, tornando essencial a discussão de outros critérios.

Ulteriormente, o texto explora o impacto das normas europeias, como o GDPR, que têm influenciado padrões de proteção de dados em escala global.

O Capítulo 4 aborda a efetividade do direito à privacidade no contexto da transferência internacional de dados pessoais, com ênfase na regulação brasileira estabelecida pela Lei Geral de Proteção de Dados (LGPD) e pela Resolução nº 19/2024 da Autoridade Nacional de Proteção de Dados (ANPD).

O capítulo traz um diagnóstico sobre o impacto dessas regulamentações na efetividade do direito à privacidade. Argumenta-se que, embora as normas busquem garantir a proteção dos titulares, sua aplicação prática tende a ser limitada por sua ênfase em formalidades contratuais e pela dependência de critérios de adequação baseados em compatibilidade jurídica, sem considerar aspectos mais amplos.

Finalmente, o capítulo aponta que a legislação brasileira, embora avance significativamente no tema da transferência internacional de dados, ainda enfrenta percalços para garantir uma proteção efetiva e substantiva à privacidade. O capítulo

destaca que há necessidade de uma abordagem mais integrada e robusta, que vá além de salvaguardas contratuais, para enfrentar as novas ameaças à privacidade em escala global.

A dissertação lida com as seguintes hipóteses: I) o estudo dos postulados fundamentais do Direito à Proteção de Dados Pessoais proporcionará *insights* valiosos para a regulação das transferências internacionais de dados, revelando aspectos cruciais sobre a efetividade do Direito à Privacidade; (II) a compreensão dos aspectos jurisdicionais envolvidos, bem como dos padrões jurídicos do GDPR e dos padrões de dados da América Latina, permitirá identificar dilemas de efetividade do direito à privacidade; (III) a análise da Lei Geral de Proteção de Dados Pessoais do Brasil exporá se a abordagem regulatória nacional é suficiente ou não para proteger a transferência internacional de dados pessoais; (IV) a investigação das práticas regulatórias nacionais, estrangeiras e internacionais e de concepções aliadas auxiliarão na determinação de uma maior efetividade para o Direito à Privacidade no Brasil.

Ao final do trabalho, em resposta à problemática da pesquisa, com o cumprimento dos objetivos traçados e a confirmação das hipóteses, chegou-se às seguintes conclusões: há uma evidente falta de uma política sólida em defesa do Direito à Privacidade. O vácuo de ferramentas fundamentais, como revisões periódicas e estatutos de bloqueio, além da negligência em tratar questões jurisdicionais e regionais, torna a LGPD e o regulamento insuficientes e frágeis. Ademais, a falta de atenção à relevância internacional e regional do Direito à Privacidade, juntamente com a inexistência de iniciativas para promover parcerias e cooperação na América Latina ou adequação jurídica regional, revela um descompromisso em assegurar uma proteção robusta à privacidade através da interoperabilidade. Tal cenário posiciona o Brasil como um território permissivo para violações de dados, comprometendo os direitos dos titulares.

2 FUNDAMENTOS DA PROTEÇÃO DE DADOS

2.1 O DIREITO À PRIVACIDADE

O termo ‘‘privacidade’’ deriva do latim *privare*, que significa excluir algo do domínio público e inseri-lo no privado (SLOOT, 2017b). Dessa forma, *privare* estabelece uma distinção em relação ao *publicare* (SLOOT, 2017b). Essa visão inicial do direito à privacidade é fulcral, pois marca o cerne das suas primeiras aplicações jurídicas como um direito fundamental para o exercício das liberdades negativas (SLOOT, 2017b).

Adrienn Lukács (2016), ao discutir a história do direito à privacidade, destaca a dificuldade de exercer a privacidade nas sociedades antigas, devido à supressão das liberdades individuais e da autonomia, resultante de uma vida orientada pelo interesse público. A urbanização do século XIX, que gerou grandes aglomerações de pessoas, foi suficiente para renovar a cosmovisão da sociedade, passando-se a privilegiar o direito à privacidade devido ao incômodo do sujeito, na sua individualidade, em viver cercado por muitos indivíduos nos crescentes contingentes populacionais urbanos (LUKÁCS, 2016). Em suma, o direito à privacidade nasce de maneira expressiva no contexto do liberalismo jurídico clássico (LUKÁCS, 2016; DONEDA, 2006).

Entretanto, é necessário adicionar um parêntese na afirmativa de Lukács (2016) e Doneda (2006), uma vez que James Weeks (1963) expõe que a origem do direito à privacidade também pode ser encontrada no direito romano, devido ao tratamento jurídico conferido à injúria pelas Leis das XII Tábuas, através da *actio aestimatoria iniuriarum*. É essa visão inicial do direito da personalidade incentivou a formatação de diversos códigos civis ocidentais modernos (WEEKS, 1963). Por outro lado, Rengel (2013) menciona registros ainda mais antigos do direito à privacidade, como o art. 21 do Código de Hamurabi (1750-1700 a.C.), o Alcorão, a Bíblia, a China Antiga, a Lei Judaica e a Grécia Antiga.

Considerado o principal marco na consolidação do direito à privacidade,[1] o artigo “*The Right to Privacy*”, publicado em 1890 na *Harvard Law Review* e escrito por Samuel Warren e Louis Brandeis, destaca a preocupação de proteger o direito à

[1] Cancelier (2017) descreve esse artigo como o primeiro marco na concepção do direito à privacidade como um direito autônomo.

privacidade diante da intensificação dos veículos de imprensa, que invadiam continuamente a vida e as experiências dos indivíduos de maneira abusiva (LUKÁCS, 2016; NISSIM; WOOD, 2018; ROUVROY; POULLET, 2009).

O direito à privacidade, conforme discernido por Samuel Warren e Louis Brandeis, constituía-se como um "*right to be let alone*", ou seja, o "direito de ser deixado em paz" (SCHREIBER, 2014; BIONI, 2014; LUKÁCS, 2016; ROUVROY; POULLET, 2009;WARREN; BRANDEIS, 1890; PETRY; HUPFFER, 2024). Nessa concepção, o "*right to be let alone*" mantinha uma relação simbiótica com o direito à propriedade (SCHREIBER, 2014; LUKÁCS, 2016; PETRY; HUPFFER, 2024).

No contexto do ''*The Right to Privacy*'' de Samuel Warren e Louis Brandeis, o direito à privacidade ganha força para proteger a burguesia dos escândalos comercializados pela imprensa (SCHREIBER, 2014; PETRY; HUPFFER, 2024). Aborda-se tal questão de forma mais enfática devido à sua relevância sociojurídica, pois o direito à privacidade não era concebido como algo acessível aos pobres, ou seja, não era visto como um direito inerente a todos os indivíduos (SCHREIBER, 2014; DONEDA, 2006; CANCELIER, 2017; RODOTÀ, 2009; PETRY; HUPFFER, 2024).

O aumento na circulação de dados e informações a partir da década de 1960 exigiu uma nova abordagem para o direito à privacidade (SLOOT, 2017b). Com isso, o direito à privacidade passou a ser entendido de forma mais ampla, fundamentado no princípio da dignidade da pessoa humana (RAMIRO, 2022; SCHREIBER, 2014). A nova concepção de privacidade se distingue do ''*right to be let alone*'', originalmente orientado pelo direito à propriedade (SCHREIBER, 2014), ao incorporar a ideia de que a vida do sujeito não é um mero patrimônio a ser gerido pelas engenharias tecnológicas (TERWANGNE, 2022).

Todavia, para melhor compreender a questão destacada no parágrafo anterior, pode-se dizer que o Direito à Privacidade consegue ser compreendido a partir de duas visões que condensam juridicamente suas funções conteudística e histórica: a visão reducionista e a visão não-reducionista. No entendimento reducionista do direito à privacidade, este se origina estritamente do conjunto de direitos à propriedade (MOORE, 2008; RENGEL, 2013). Por outro lado, a compreensão não-reducionista considera que a privacidade deriva de outros direitos, destacando os elementos socioeconômicos, culturais, políticos e antropológicos

como influenciadores significativos do que é concebido como privacidade em uma determinada sociedade (MOORE, 2008; LUKÁCS, 2016; KUNER, 2010c; KUNER, 2009b).

A visão reducionista da privacidade tem marcado a história das constituições do Brasil, aparecendo na Constituição de 1824 como o direito à inviolabilidade domiciliar (DONEDA, 2006). Historicamente, a privacidade no Brasil foi caracterizada por sua associação com a propriedade (DONEDA, 2006). Com a despatrimonialização ou repersonalização das relações privadas (NETO, 2013; SILVA; NASCIMENTO; COSTA, 2024), introduzida pela Constituição Federal de 1988, a concepção brasileira de privacidade se afastou de uma visão estritamente patrimonialista, passando a valorizar outros direitos além da propriedade (NETO, 2013; MOORE, 2008; DONEDA, 2006; NASCIMENTO; COSTA, 2023; SILVA; NASCIMENTO; COSTA, 2024).

A concepção jurídica reducionista da privacidade foi superada na sociedade pós-industrial com o surgimento do *Welfare State*, que valorizava menos o individualismo (DONEDA, 2006; SLOOT, 2017b). Foi necessário conferir uma nova abordagem ao direito à privacidade para atender aos diversos interesses na sociedade (DONEDA, 2006; FARNASIER; KNEBEL, 2021; SLOOT, 2017b).

Com a digitalização da sociedade, que permeia todos os aspectos da vida no ambiente virtual (SILVA; NASCIMENTO, 2023), surge um dilema para o direito à privacidade: a própria associação com a propriedade, que originalmente fundamentou esse direito, torna-se, contemporaneamente, um dos principais obstáculos para seu exercício (DONEDA, 2006). Se a privacidade é equiparada à propriedade, ela pode ser negociada como tal (FARNASIER; KNEBEL, 2021). Dessa forma, entende-se por qual razão, atualmente, o direito à privacidade tem se transformado em um “direito negociável’’ (TUBARO, 2018; FARNASIER; KNEBEL, 2021).

Em continuidade, Bart van der Sloot (2017b) e Bioni (2014) afirmam a tradição do direito à privacidade como um direito negativo, focado na liberdade. À vista disso, Doneda (2006), Bioni (2014) e Sloot (2017b) questionam a concepção de que o direito à privacidade seja apenas um direito subjetivo. Diante dos recentes desenvolvimentos sociais, econômicos e legais, é possível começar a entender o direito à privacidade em uma dimensão positiva (BIONI, 2014). Essa abordagem

assume características específicas, como a preocupação com a proteção dos dados pessoais dos trabalhadores, indo além da concepção individual do direito à privacidade (TUBARO, 2018).

Dessa forma, a vida privada é inserida dentro da esfera social de proteção de direitos (TUBARO, 2018). A citada inflexão descreve a interação entre duas concepções de privacidade: a norte-americana e a europeia (HEUVEL; HOBOKEN, 2022). À vista disso, o direito à privacidade norte-americano centra-se na proteção individual, enquanto o direito à privacidade europeu destaca-se pelo envolvimento com a dignidade da pessoa humana (HEUVEL; HOBOKEN, 2022; SLOOT, 2017b). A supramencionada diferença é especialmente perceptível porque, enquanto a União Europeia adota uma proteção de dados baseada em direitos (BROWNSWORD, 2009), os Estados Unidos fundamentam sua abordagem de privacidade na ocorrência de danos, com foco na maior liberdade de mercado (HEUVEL; HOBOKEN, 2022).

Dessarte, se a despatrimonialização do direito à privacidade ocorre em função do princípio da dignidade da pessoa humana, que orienta tais relações, é relevante destacar a importância de, apesar das mudanças contemporâneas, ainda conceber o direito à privacidade como um direito individual para garantir o próprio sucesso da dignidade da pessoa humana (GONZALBO, 2004). Afinal, seria impossível assegurar a dignidade da pessoa humana sem a liberdade (GONZALBO, 2004), porque é o no exercício da individualidade que residem os direitos da personalidade.

Rubenfeld (1989) destaca que os direitos da personalidade são frequentemente considerados sinônimos ou subjacentes ao direito à privacidade. Sloot (2017b), no entanto, faz um adendo e descreve o direito à privacidade como distinto dos direitos da personalidade. Assim, enquanto o direito à privacidade determina estritamente a ocultação do sujeito para protegê-lo, o direito da personalidade pode atuar tanto ocultando quanto exibindo o sujeito (SLOOT, 2017b), protegendo-o de ambas as formas.

Partindo do pressuposto de que o direito da personalidade é o direito à autodefinição, surge a questão de como avaliar juridicamente quais autodefinições merecem tutela do direito à privacidade (RUBENFELD, 1989). O fator da identidade é central nessa questão, cujo problema reside em fazer um juízo moral, e não normativo, acerca de determinadas identidades (RUBENFELD, 1989). Rubenfeld

destaca que o fator “dano’’ possui uma maior objetividade do que o fator “identidade’’. Assim, as pessoas podem exercer livremente os direitos da personalidade, desde que não causem danos a terceiros (RUBENFELD, 1989).

Rubenfeld (1989) também descreve que, embora o dano seja um critério mais objetivo do que a identidade, ele não deixa de ser igualmente problemático, pois há questões que são de interesse da sociedade. Um exemplo disso é o assédio sexual, que não pode ser protegido pelo direito à privacidade.

Nesse caso, surge a contraposição entre a crítica liberal e a crítica republicana do direito da personalidade (RUBENFELD, 1989). Assim, quanto à crítica liberal e a crítica republicana do direito da personalidade, aplicadas ao Direito à Privacidade, observa-se uma evolução marcante de tais perspectivas no Direito Norte-Americano.

Dito isso, no Direito Estadunidense, o caso *Griswold v. Connecticut* inaugurou a discussão sobre o direito à privacidade ao combater estatutos que proibiam o uso e a distribuição de preservativos (RUBENFELD, 1989). Na decisão, a Suprema Corte argumentou que as decisões íntimas de um casal dizem respeito exclusivamente a eles, e não ao Estado (RUBENFELD, 1989). É importante destacar que, na decisão *Griswold v. Connecticut*, o direito à privacidade foi mencionado como um direito fundamental implícito, atuando na penumbra dos direitos declarados (RENGEL, 2013).

No mesmo sentido, o caso *Loving v. Virginia* pôs fim à proibição de casamentos interraciais, afirmando que questões de foro íntimo não são de competência estatal (RUBENFELD, 1989). Aqui, é possível observar a perspectiva substancial da privacidade indicada por Anderson Schreiber (2014), na qual o direito à privacidade se configura como um instrumento jurídico que desconsidera os valores morais, mesmo em uma sociedade altamente dividida racialmente e que professe essa estratificação social (RUBENFELD, 1989). Em adição, a efetividade do direito à privacidade na crítica liberal dos direitos da personalidade afirma: existe liberdade fora do controle.

Por conseguinte, no caso *Eisenstadt v. Baird*, houve a extensão do direito de usar preservativos para pessoas solteiras, indo além do que foi decidido em *Griswold v. Connecticut* (RUBENFELD, 1989). Em *Roe v. Wade*, a Corte definiu que a amplitude do direito à privacidade abrange a intimidade da decisão pelo aborto, não

sendo esta, portanto, uma decisão tutelada pelo Estado (RUBENFELD, 1989). Em *Moore v. Cidade de East Cleveland*, a Corte dos EUA firmou o entendimento de que o Estado não pode intervir em assuntos familiares (RUBENFELD, 1989).

Entretanto, invocando a crítica republicana dos Direitos da Personalidade, no caso *Bowers v. Hardwick*, a Suprema Corte dos EUA afirmou a constitucionalidade da lei de sodomia da Geórgia, especialmente em relação às práticas sexuais homoafetivas, numa votação apertada de 5-4 (RUBENFELD, 1989).

Assim, a partir do caso *Bowers v. Hardwick*, observa-se como essa discussão reverbera no direito à privacidade, uma vez que os magistrados que votaram pela constitucionalidade da Lei de Sodomia argumentaram que os direitos da personalidade devem basear-se na autodefinição da sociedade, que naquele momento tinha valores homofóbicos – segundo os julgadores –, sustentando a constitucionalidade com base na visão republicana dos direitos da personalidade (RUBENFELD, 1989). Por outro lado, a parte vencida da Suprema Corte, fundamentando-se na visão liberal dos direitos da personalidade, afirmou a inconstitucionalidade da Lei de Sodomia, argumentando que os direitos da personalidade correspondem ao desenvolvimento individual, mesmo que de forma incompatível com os valores da sociedade (RUBENFELD, 1989).

O caso *Bowers v. Hardwick* foi superado pelo caso *Lawrence v. Texas* (2003), privilegiando-se, neste último, o princípio liberal da personalidade na análise do Direito à Privacidade (autodefinição pessoal), em detrimento do princípio republicano dos Direitos da Personalidade (autodefinição coletiva) (RUBENFELD, 1989; RENGEL, 2013). As relações homoafetivas deixaram de ser categorizadas como uma ofensa jurídica a partir de uma interpretação fundamentada na 4ª Emenda da Constituição dos EUA, declarando-se inconstitucional a lei do Texas que proibia relações sexuais homoafetivas (RENGEL, 2013).

Em resumo, a crítica republicana ao direito da personalidade busca contrapor a ideia de que o direito à personalidade implique a possibilidade de desenvolvimento com base em valores individuais, que podem, em algum nível, se opor aos valores da sociedade (RUBENFELD, 1989). Em contraste com a cosmovisão individualista da personalidade, a visão republicana compreende o direito da personalidade a partir de uma perspectiva coletiva de direito (RUBENFELD, 1989).

Rubenfeld (1989) destaca que não pode haver confusão entre a vontade de uma sociedade de ser governada por determinados códigos sociais e a identidade individual. A identidade só pode ser emanada no seio da individualidade, pois afirmar que a autodefinição da personalidade deve ocorrer apenas com base em pressupostos coletivos é negar a possibilidade de exercício da individualidade no âmbito de uma sociedade, o que tornaria a ordem jurídica extremamente autoritária (RUBENFELD, 1989).

Segundo Jed Rubenfeld (1989), há um problema de ordem normativa nos direitos da personalidade, pois, se a personalidade baseada na identidade for juridicamente neutra, ela também deverá proteger aqueles que são intolerantes como um aspecto indispensável da personalidade.

Rubenfeld (1989) descreve que essa questão é facilmente resolvida quando o direito estabelece que ser intolerante em relação às decisões de outras pessoas não deve ser constitucionalmente tutelado, pois não é algo essencial para a personalidade de alguém. Nesse contexto, o direito à privacidade se torna um elemento imprescindível para proteger o âmago liberal dos direitos da personalidade, porque a proteção da vida privada repele as interferências de terceiros ou da sociedade na autodefinição individual (RUBENFELD, 1989).

Assim, não haveria um livre desenvolvimento da personalidade em ser preconceituoso, nem haveria liberdade no desenvolvimento da personalidade se ela fosse limitada pelas condições da sociedade (RUBENFELD, 1989). Rengel (2013) destaca o direito à privacidade como sendo caracteristicamente inato, um *locus* de liberdade onde os sujeitos desenvolvem suas identidades sem a intervenção de outros.

Outrossim, é possível afirmar que o direito à privacidade foi significativamente construído a partir das conquistas jurídicas da comunidade LGBTQ+ e, de maneira mais ampla, das lutas por liberdade sexual, sendo frequentemente invocado no Tribunal Europeu de Direitos Humanos (TEDH) para combater as leis anti-homossexualidade em países europeus, como nos casos *Dudgeon* v. Reino Unido, *Norris v.* Irlanda, *Lustig-Prean & Beckett v.* Reino Unido, Salgueiro da Silva Mouta v. Portugal, *Modinos* v. Chipre, *Van Kück* v. Alemanha, entre outros (RENGEL, 2013), e nos casos mencionados acima na Suprema Corte dos EUA.

Seguindo a discussão sobre o Direito à Privacidade, distintamente da evolução histórica do Direito à Privacidade nos EUA, segundo James Weeks (1963), os tribunais ingleses não consideravam o direito à privacidade como um direito juridicamente autônomo, mas sim como um direito parasitário, que orbitava em torno de outros direitos — como os direitos contratual, de propriedade, autoral, entre outros — mas nunca assumia a centralidade como um direito independente e fundamental.

Segundo James Weeks (1963) e Rengel (2013), no direito consuetudinário inglês, os tribunais sempre evitaram mencionar o direito à privacidade como algo juridicamente relevante. No caso *Gee v. Pritchard*, houve a concessão de uma liminar para impedir a publicação de cartas, não por se tratar de uma violação da intimidade, mas porque as cartas faziam parte do acervo da propriedade do sujeito tutelado na ação (WEEKS, 1963). No entanto, em 1961, houve uma tentativa na Câmara dos Lordes do Reino Unido de fazer viger o *"The Right of Privacy Bill"*, que não foi aprovado (WEEKS, 1963). Esse cenário foi alterado em 1998, com a aprovação da Lei de Proteção de Dados e da Lei de Direitos Humanos do Reino Unido (RENGEL, 2013).

Em 1900, a justiça francesa decidiu, em um caso envolvendo um retrato em pintura, que o sujeito retratado tem direito à sua imagem, enquanto o pintor tem direito à sua obra, não podendo este último publicar a obra de forma que a pessoa retratada seja identificável, a menos que tenha o consentimento da pessoa retratada (WEEKS, 1963). Em 1970, o direito à privacidade foi introduzido com maior robustez no Código Civil francês (RENGEL, 2013).

No direito latino-americano, Rengel (2013) descreve que o registro mais antigo do direito à privacidade advém da Constituição da Argentina de 1853. No entanto, esse dado deve ser retificado, uma vez que a Constituição do Brasil de 1824 precede a Constituição argentina de 1853 em algumas décadas, e naquele momento continha disposição sobre a inviolabilidade domiciliar. A Constituição mexicana de 1917, segundo Rengel (2013), também dispôs sobre privacidade, assegurada pela Ação de Amparo. Em 1996, o México introduziu na Constituição a proteção às comunicações privadas, seguindo a orientação do direito à inviolabilidade domiciliar presente na Constituição mexicana de 1856 (RENGEL, 2013).

No geral, o entendimento inicial do Direito Inglês, que é dissonante com a cultura Estadunidense, Europeia e Latino-americana, é minimamente curioso: seria o Direito à Privacidade um Direito? Em sentido semelhante à tal entendimento, Judith Jarvis Thomson (1975) afirmou a existência de um *cluster privacy*, sugerindo que o direito à privacidade é sobreposto por vários outros direitos, não sendo, portanto, um direito juridicamente autônomo.

Thomson (1975) destaca que o direito a não ser torturado implica, de maneira subjacente, que determinado sujeito, dentro de uma ordem jurídica, tem o direito à integridade física. Entretanto, a violação do direito à proteção de dados pessoais não significa necessariamente uma violação do direito à inviolabilidade domiciliar. Thomson (1975) argumenta que há um conjunto de direitos que são afirmados como direitos de privacidade (*cluster privacy*), mas possuir um direito não implica, de forma implícita, que todos os outros direitos serão afetados por uma violação específica. Assim, quando ocorre uma violação do direito à proteção de dados, isso não constitui uma violação do direito à privacidade em sua totalidade, mas sim de um direito específico à proteção de dados pessoais, de um direito de propriedade ou de um direito inerente à própria pessoa (ROESSLER, 2017).

Para Thomson (1975), não existe uma ideia muito clara do que seja o direito à privacidade, exceto que ele consiste em um grupo de direitos (*cluster privacy*), composto por direitos totalmente diferentes entre si, que têm em comum apenas o fato de pertencerem a esse grupo. À vista disso, o direito à privacidade não é visualizado em primeiro plano; primariamente, há a identificação de uma violação de um direito específico mais imediato (THOMSON, 1975; ROESSLER, 2017).

Assim, quando um dado sensível, no direito brasileiro, é coletado sem o consentimento do titular, a violação imediata que se percebe é a violação da proteção de dados pessoais e, secundariamente, afirma-se que houve uma violação da privacidade, considerando que o direito à proteção de dados pessoais faz parte do *cluster privacy*.

As deduções feitas a partir da perspectiva de Thomson (1975) podem aparentemente oferecer um afago à emanação da privacidade. No entanto, elas também apresentam um dilema jusfilosófico intransponível.

Nesse ínterim, se a privacidade se firma como uma base comum da qual direitos são percebidos como participantes (*cluster privacy*), então é a partir desse

aspecto conclusivo comum que direitos específicos são constituídos (ROESSLER, 2017).

Mas qual seria, por exemplo, o *a priori* do direito à proteção de dados pessoais? Qual norma o reconhece como um direito justificado e legítimo? Sem o sentido normativo, subjacente e precedente da proteção à privacidade, não é possível criar um sentido *a posteriori*, normativo e expresso, que se convalide como direitos específicos, unívocos, autossuficientes e com um fim em si mesmos. Portanto, a privacidade não pode ser apenas um *cluster privacy*; ela pode ser concebida substancialmente *a priori*, subjacendo a esses direitos específicos (ROESSLER, 2017).

Bruno Bioni (2017) descreve que os direitos derivados da privacidade estão intrinsecamente ligados à estrutura física que os fundamenta. Assim, a privacidade funda tais direitos e é também a conclusão desses direitos, sendo os direitos específicos mais imediatos os meios pelos quais o direito à privacidade é efetivado, mas não um fim em si mesmos (ROESSLER, 2017). Isso ocorre porque a privacidade é um conceito dinâmico que se adapta a diferentes contextos e ambientes (ROESSLER, 2017; BIONI, 2017), seja no espaço físico, digital ou social. Por isso, é natural que ela se transforme conforme as mudanças de ambiente, refletindo as necessidades e expectativas de cada situação (ROESSLER, 2017). Assim, o fato de existirem diferentes direitos de privacidade ou interpretações sobre ela não significa que a privacidade deixe de existir (ROESSLER, 2017).

Os direitos intermediários são a formalidade pela qual o direito à privacidade será cumprido e, ao mesmo tempo, a formalidade que surge da preocupação substancial *a priori* com a proteção da privacidade. Dessa forma, o direito à privacidade é o começo e o fim em si mesmo, cuja efetividade enquanto direito fundamental se dá pelo cumprimento de Direitos intermediários e específicos.

Nesse ínterim, segundo Schreiber (2014), há uma dupla dimensão da privacidade, abrangida por aspectos formais e substanciais. Na dimensão formalista da privacidade, fala-se, por exemplo, do devido tratamento de dados pessoais, ou seja, se o tratamento de dados foi realizado conforme os procedimentos estabelecidos pela Lei Geral de Proteção de Dados Pessoais.

Schreiber (2014, p. 140) afirma que “a dimensão procedimental da privacidade se exprime, em primeiro lugar, na coleta da informação pessoal. A coleta

clandestina ou desautorizada de informações pessoais deve ser repelida''. É nesse contexto que surge a necessidade do devido tratamento de dados pessoais, ou seja, que a coleta, gestão e descarte de dados pessoais sejam realizados conforme preconiza a Lei Geral de Proteção de Dados Pessoais.

Quanto à dimensão substancial, esta está relacionada aos objetivos que se têm com o "[...] uso (...) do dado pessoal, o que implica, muitas vezes, em violações a outros direitos da personalidade'' (SCHREIBER, 2014, p 140). Consoante Negri e Korkmaz (2019, p. 74) "o dado pessoal sensível é delimitado por intermédio de eixos de *fattispecie*, ou seja, através de um esquema taxativo e, portanto, limitado de situações jurídicas objetivas''. Dessa forma, os dados sensíveis "[...] estão associados às opções e características fundamentais da pessoa humana, de forma a se destacarem pela aptidão de gerar situações de discriminação e desigualdade'' (NEGRI; KORKMAZ, 2019, p. 67). Se um dado sensível é um recorte imprescindível da personalidade de determinado sujeito (FRANCO, 2009), exige-se um maior rigor com a sua proteção (NEGRI; KORKMAZ, 2019; TRAN, 2020).

Em resumo, a Lei Geral de Proteção de Dados Pessoais e a Autoridade Nacional de Proteção de Dados (ANPD) contemplam dispositivos que se ocupam da privacidade em sua dimensão substancial, com o princípio antidiscriminatório de dados pessoais (art. 5º, XI, da LGPD) e o direito de acesso de informações pelo titular acerca do tratamento de dados pessoais (art. 9º, *caput*, da LGPD). Estes dispositivos não estão relacionados exatamente ao cumprimento do devido tratamento de dados pessoais, mas sim em impedir consequências da violação da privacidade, freando sua instrumentalização para fins discriminatórios e assegurando ao titular do dado pessoal o poder de vigilância sobre o tratamento de dados pessoais.

Quando James Weeks (1963) afirma que o Direito à Privacidade nasce a partir de Brandeis e Warren com o objetivo primordial de conter os veículos de comunicação para que não houvesse o cerceamento total da liberdade individual da burguesia, a necessidade de conter a interferência nas liberdades individuais (RENGEL, 2013; DONEDA, 2006) e, agora, coletivas (DONEDA, 2006), das Tecnologias de Informação e Comunicação, expõe como o Direito à Privacidade continua mantendo a preocupação que lhe deu origem.

Adam D. Moore (2008) defende que a privacidade seja definida a partir da ideia de “controle”. Assim, seria juridicamente atribuído ao sujeito o poder de manipular bens que são intangíveis e, consequentemente, inerentes à sua personalidade (MOORE, 2008).

Há, ainda, a doutrina de que a privacidade deve ser medida pelas expectativas de privacidade (SCHREIBER, 2014; ROUVROY; POULLET, 2009). No entanto, essa visão é criticada por ser menos protetiva do que a perspectiva do direito à privacidade definida pela dignidade da pessoa humana (ROUVROY; POULLET, 2009). Por exemplo, mesmo quando câmeras são colocadas em ambientes de trabalho para avaliar a produtividade em tempo real, e os funcionários têm ciência de que estão sendo monitorados, tudo o que é pessoal é completamente perdido (ROUVROY; POULLET, 2009).

As perspectivas elucidadas são importantes, porém, dada a atual experiência dos sujeitos com as tecnologias de informação e comunicação, é possível inferir que o controle, como um instrumento de autodeterminação informativa e a privacidade definida em níveis de expectativa, enfrentam limitações cognitivo-decisórias dos usuários e problemas de vigilância excessiva, conforme defendem Laura Schertel Mendes e Gabriel C. Soares (2020), especialmente no que se refere à capacidade de estabelecer um consentimento informado na coleta de dados.

Na contemporaneidade, percebe-se uma violação sistemática e generalizada do direito à privacidade, decorrente dos avanços nas tecnologias de informação e comunicação. Segundo Bart van der Sloot (2017b), a privacidade na contemporaneidade, coletivizada através da categorização de infinitos dados, relaciona-se tanto à proteção de grupos vulnerabilizados (SILVA; NASCIMENTO, 2023) quanto ao entendimento jurídico desse direito como fundamental para assegurar a ordem pública e a segurança nacional (SILVA; NASCIMENTO; ROSA, 2023; SLOOT, 2017b).

Sloot (2017b) aborda o conceito de privacidade de grupo, que surge como uma crítica à privacidade excessivamente voltada para o sujeito individual. Diante dessa urgência, Lee A. Bygrave e Dag Wiese Schartum (2009) abordam o consentimento de grupo é imprescindível para garantir o Direito à Privacidade. No contexto em questão, o consentimento coletivo implica a autorização de uma decisão tomada em grupo, na qual os titulares de dados não são chamados a aprovar

individualmente cada ato específico (BYGRAVE; SCHARTUM, 2009). Esse modelo estabelece uma escolha comum, que se torna obrigatória para todos os membros do grupo, independentemente de eventuais discordâncias de alguns participantes em relação à decisão tomada (BYGRAVE; SCHARTUM, 2009). Diante dos novos paradigmas tecnológicos, é complicado pensar que o sujeito, em sua individualidade, conseguirá se impor contra corporações poderosas – como a Meta – que desafiam até o poder do Estado-nação (ANDREWS, 2020), descentralizando a soberania estatal (MENDES; FERNANDES, 2020).

Os instrumentos de transparência no tratamento de dados são juridicamente contraproducentes, pois, antes de qualquer coisa, o sujeito precisa estar ciente de que sua privacidade está sendo indevidamente violada, algo extremamente difícil de se descobrir nas Novas Tecnologias de Informação e Comunicação (SLOOT, 2017b). E, relativamente ao consentimento, Laura Schertel Mendes e Gabriel C. Soares (2020) abordam as limitações cognitivo-decisórias do usuário, destacando uma série de fatores, como: I) interesse social inesquivável; II) falta de conhecimento técnico do contratante em relação aos termos, condições e permissões.

Dito isso, Sloot (2017b) está correto ao destacar que a privacidade focada no sujeito, na era das tecnologias de informação e comunicação, é dificilmente efetiva, sendo os próprios instrumentos jurídicos uma forma de legalização da economia invasiva (SILVA; NASCIMENTO; ROSA, 2023), ou, como teorizado por Shoshana Zuboff (2015; 2021), do capitalismo de vigilância.

Sloot (2017b) dá ênfase a essa discussão ao destacar vertentes cruciais para entender a ausência de efetividade na lógica individualista da proteção de dados pessoais. No caso do princípio *ratione personae*, Sloot (2017b) expõe seu declínio, argumentando que, à medida que as violações dos direitos de privacidade se tornam cada vez mais coletivizadas, não é possível que um sujeito reclame uma violação personalíssima. Isso ocorre porque as violações de direitos tornam-se gradualmente abstratas, como consequência de um esvaziamento dos interesses individuais em favor dos interesses econômicos gerais.

Assim, no princípio *ratione materiae*, Sloot (2017b) descreve que, quando ocorre uma violação de proteção de dados pessoais, ao consultar a matéria a esse respeito, observa-se que o dado só será considerado violado se estiver relacionado a uma pessoa física identificada ou identificável. Todavia, Sloot (2017b) argumenta

que, na era da sociedade da informação, os dados pessoais são frequentemente agrupados, ou seja, não são manuseados na esfera individual, o que impede o alcance de uma proteção de dados que só pode ser invocada quando há pessoalização, ou seja, a individualização do dado pessoal. Esses dados, quando instrumentalizados, podem alterar substancialmente o ambiente e os serviços usados por um cidadão, tornando o impacto juridicamente relevante (SLOOT, 2017b). Portanto, o conceito de dados pessoais e a própria noção de proteção de dados são questionáveis para fins de proteção.

Relativamente à ponderação, Sloot (2017b) afirma que há uma negociação entre privacidade e segurança. O problema disso, na visão do autor, é que há uma definição muito concreta de segurança (SLOOT, 2017b), o que faz com que a privacidade possa ser negociada em vão, tornando difícil alcançar uma equalização adequada. Além disso, é complicado prever os interesses individuais em relação à privacidade (SLOOT, 2017b).

Bart van der Sloot (2017b) observa que o Tribunal Europeu de Direitos Humanos tem, em algumas ocasiões, abandonado a visão do direito à privacidade como sendo de natureza exclusivamente subjetiva, evitando analisá-lo apenas de forma concreta, ou seja, invocando os princípios *ratione personae* e *ratione materiae*. Nesses casos, o tribunal analisa questões como a vigilância estatal considerando o direito à privacidade de forma abstrata, sem se concentrar no interesse personalíssimo de um cidadão, mas sim no interesse coletivo. A título de exemplo, no ceio do Tribunal Europeu de Direitos Humanos (TEDH), o caso e *Ekimdzhiev* v. Bulgária questionava a discricionariedade da coleta de dados realizada pelo serviço secreto (SLOOT, 2017b). O governo contestou a reinvidicação das partes, informando que não havia a demonstração do interesse personalíssimo na reclamação. O TEDH acolheu o pedido dos reclamantes considerando a privacidade *in abstrato*, analisando apenas a probabilidade de que o dano realmente poderia ter acontecido (SLOOT, 2017b).

Em conclusão, a partir de tudo o que foi discutido, o direito à privacidade pode ser resumido em: I) Privacidade enquanto Isolamento; II) Privacidade enquanto autonomia descisória; III) privacidade enquanto autodeterminação informacional; IV) Privacidade enquanto princípio bidirecional (ROUVROY; POULLET, 2009).

No contexto da privacidade enquanto isolamento, encontra-se a concepção clássica do direito à privacidade, que busca garantir a liberdade do indivíduo ao permitir que ele se afaste juridicamente de interferências externas indesejadas, seja da sociedade, do Estado ou até de seus pares, e no lado oculto, possa desenvolver sua personalidade livremente, com escopo geográfico de aplicação (ROUVROY; POULLET, 2009). Segundo Bart van der Sloot (2017b), esse conceito está profundamente relacionado à ideia de proteção do espaço pessoal, onde o indivíduo tem o direito de ser deixado em paz, sem que sua vida íntima seja invadida ou explorada publicamente. Essa visão remonta à origem do direito à privacidade, que surgiu como uma forma de defesa contra a exposição não autorizada, conforme destacado por Schreiber (2014) e Lukács (2016), ou seja, a privacidade é a liberdade e o direito de não sofrer interferências.

A privacidade, quando entendida como autonomia decisória, baseia-se na ideia de que os indivíduos devem ter o controle total sobre suas próprias decisões e escolhas, sem que o Estado ou a sociedade imponham uma decisão pressuposta sobre elas (ROUVROY; POULLET, 2009). Se reflete, assim, uma profunda preocupação com a liberdade pessoal e com a dignidade humana, como destacam autores como Schreiber (2014) e Doneda (2006), que veem a privacidade como um pilar essencial para o pleno desenvolvimento da personalidade.

A privacidade enquanto autodeterminação informacional é crucial na era digital, e visa equilibrar o poder informacional, onde o controle sobre a informação pessoal se torna cada vez mais complexo (ROUVROY; POULLET, 2009). O direito à autodeterminação informacional implica que o indivíduo deve ser capaz de controlar todas as etapas do tratamento de seus dados, desde a coleta até o seu uso e descarte (ROUVROY; POULLET, 2009). Como discutido por Sloot (2017b) e Rouvroy e Poullet (2009), a privacidade deve ser garantida pela possibilidade de o sujeito decidir sobre o destino de suas informações pessoais, sem ser coagido ou manipulado. A privacidade não pode ser entendida como uma mera possibilidade de negociar dados pessoais, mas como um mecanismo que assegura ao indivíduo a capacidade de decidir, livre de pressões externas ou da mercantilização de suas informações (ROUVROY; POULLET, 2009).

Por fim, há a privacidade em seu aspecto principiológico bidirecional (ROUVROY; POULLET, 2009). Nesse aspecto, é possível observar que a

privacidade tanto servirá para garantir a reclusão do sujeito quanto para garantir que ele participe democraticamente em sociedade (ROUVROY; POULLET, 2009). Essa concepção bidirecional da privacidade, que assegura tanto a reclusão quanto a participação ativa em sociedade, constitui a ideia central do *Datenschutz* Alemão (SUDA, 2017).

O Direito à Privacidade é sinônimo de democracia (SUDA, 2017). Todas as Democraciais liberais regulam, em algum grau, o Direito à Privacidade e o Direito à Proteção de Dados Pessoais (SUDA, 2017). Numa democracia, o Direito à Privacidade é crucial para que os sujeitos em sociedade, através da implementação de liberdades, experimentem uma vida verdadeirmente autodeterminada (ROUVROY; POULLET, 2009). É exatamente por isso que os regimes autoritários são caracterizados pelo excesso de vigilância (ORWELL, 2019; KAFKA, 1997). O direito à privacidade e o Direito à Proteção de Dados Pessoais possuem um valor fundamental no Estado Democrático de Direito, indo além do simples interesse individual de um cidadão – são ferramentas socioestruturais essenciais para a continuidade das liberdades e da democracia (ROUVROY; POULLET, 2009).

Utilizando-se da compreensão de Dworkin (1985) para o direito à privacidade, o que implica que sua proteção transcende interesses utilitaristas e se fundamenta em um compromisso moral com a autonomia e a dignidade dos indivíduos. A abordagem de Dworkin (1985) reforça a visão de que a privacidade não é apenas um instrumento para evitar danos, mas um direito essencial para o pleno desenvolvimento da vida pessoal e social. Com base no pensamento de Dworkin (1985), pode-se dizer que a privacidade não é um privilégio ou uma prerrogativa opcional, mas um direito essencial que sustenta a própria ideia de cidadania em uma democracia.

Dito isso, far-se-á a seguinte conclusão: o direito à privacidade emerge como um conceito multifacetado, que transcende sua origem histórica vinculada à proteção da liberdade individual e à propriedade para se firmar como um alicerce essencial das democracias modernas. Desde a garantia do isolamento e da autonomia decisória até a autodeterminação informacional e a participação social, a privacidade se revela como um direito que não apenas protege o indivíduo, mas também assegura o equilíbrio entre liberdade e dignidade em uma sociedade cada vez mais interconectada e tecnologicamente avançada. Reconhecê-lo como um princípio

jurídico fundamental, e não apenas como um cluster de direitos menores, reafirma seu papel central na construção de uma ordem democrática, onde a proteção das liberdades individuais e coletivas garante tanto o desenvolvimento pessoal quanto a continuidade das instituições que sustentam a justiça e a igualdade. Assim, a privacidade, mais do que um direito isolado, é a base de um compromisso moral com a preservação da autonomia e da dignidade humanas, sendo imprescindível para a realização de uma sociedade verdadeiramente livre e democrática.

2.2 O DIREITO À PROTEÇÃO DE DADOS PESSOAIS E A CONSTITUCIONALIZAÇÃO DO DIREITO NO BRASIL

No âmbito da União Europeia, entende-se por dado pessoal o dado indentificado ou identificável referente à pessoa natural, ou seja, compreende-se os aspectos diretos e indiretos da tutela aos dados pessoais (TERWANGNE, 2022; MATTO; MELTZER, 2018). O termo proteção de dados deriva do alemão *Datenschutz*, que significa privacidade em um sentido político, ou seja, que tenta conciliar o direito à privacidade ao mesmo tempo em que permite o uso controlado de tais informações, por procedimentos que mantenham incólume o direito à privacidade (SUDA, 2017).

O Direito à Proteção de Dados Pessoais tem como núcleo o princípio da autodeterminação informativa e o princípio do livre desenvolvimento da personalidade (ROUVROY; POULLET, 2009; SILVA; NASCIMENTO; COSTA, 2023). Carolina Mendes Franco (2009) argumenta que, à medida que a coleta de dados se expande, surge a preocupação com a proteção dos dados pessoais – a sociedade percebe a necessidade de um direito na ausência deste. As dinâmicas de coleta de dados envolvem uma lógica de apropriação na qual o sujeito é privado de sua própria identidade (SILVA; NASCIMENTO, 2023). Esta perspectiva, inserida em um contexto jurídico que busca constitucionalizar-se (COSTA, 2019), como é o caso do Brasil, apresenta um dilema a ser enfrentado. Em outras palavras, enquanto as lógicas de apropriação de dados representam uma mercantilização da vida do sujeito (SILVA; NASCIMENTO, 2023; SILVA; NASCIMENTO; COSTA, 2023), a constitucionalização do Direito, e sua consequente gama de Direitos Fundamentais,

sugere a necessidade de desmercantilizar ou repersonalizar o sujeito nos âmbitos privado, público e social (NETO, 2013; BORGES, 2007; LAFER, 1988).[2]

À medida que relações de poder tentam alienar o sujeito de si mesmo, desviando-o do controle de sua própria vida (SILVA; NASCIMENTO; LIMA, 2024), a proteção de dados pessoais tenta reavivar a ideia de que o sujeito é o dono de si mesmo e precisa assumir o controle de sua própria existência (BORGES, 2007). Dessa forma, "[...] o direito à intimidade visa salvaguardar do conhecimento alheio e sinais mais profundos do ser, da vivência e dos sentimentos, e se encontra em risco diante da circulação de dados pessoais'' (BELTRÃO; MENEZES, 2019, p. 1413).

Segundo Silvio Romero Beltrão (2013, p. 208), "os direitos da personalidade são absolutos em face do seu caráter *erga omnes*, em que a sua atuação se faz em toda e qualquer direção, sem a necessidade de uma relação jurídica direta para se respeitar este direito''.

Essa característica pode ser vista em dois momentos. No primeiro momento, a partir do artigo 1º da Lei Geral de Proteção de Dados, quando deixa claro que um dos objetivos da lei é assegurar o livre desenvolvimento da personalidade, justificando sua inclusão como princípio norteador da proteção de dados pessoais no art. 2º, VII. E, no segundo momento, a concepção de Beltrão (2013) é reforçada pelo surgimento da Emenda Constitucional nº 115/2022 como indicativo do compromisso com a constitucionalização da proteção de dados pessoais, vinculando todos os agentes no cumprimento do Direito à Privacidade (SILVA; NASCIMENTO; COSTA, 2023; SILVA; NASCIMENTO; ROSA, 2023). Assim, um instituto que era tradicionalmente tratado "[...] nos códigos privados (família, propriedade, etc.) passaram a serem disciplinados também nas constituições contemporâneas (...) é o fenômeno chamado (…) de relevância constitucional das relações privadas'' (NETO, 2013, p. 29).

Com a introdução de tecnologias de informação e comunicação, os dados pessoais se tornaram um importante ativo financeiro (SILVA; NASCIMENTO; ALMEIDA, 2023; SILVA; NASCIMENTO; LIMA, 2024; BIONI, 2014), e a catalogação

[2] Ainda que Eugênio Facchini Neto (2013) não tenha se referido diretamente à constitucionalização da proteção de dados pessoais, mas sim à constitucionalização do direito privado, um trecho de um de seus artigos mais notáveis pode ser interpretado, ainda que de forma extemporânea, à luz do contexto apresentado. Nas palavras do autor, a constitucionalização do direito privado pode ser vista como a ''[...] repersonalização do direito civil, ou visto de outro modo, a despatrimonialização do direito civil. Ou seja, recoloca-se no centro do direito civil o ser humano e suas emanações'' (NETO, 2013, p. 26).

dos corpos ganhou notabilidade (SILVA; NASCIMENTO, 2023), sugerindo existências ainda mais vulneráveis e distantes da dignidade humana (art. 1º, III, CRFB/88) (FRANCO, 2009).

A redução da pessoa humana a um mero dado representa uma ameaça ao princípio da dignidade humana e do livre desenvolvimento da personalidade, direitos que reconhecem o sujeito em sua completude, diversidade e subjetividade (FRANCO, 2009). Segundo Schreiber (2014, p. 139-140), “toda a complexidade da pessoa humana, em sua singular individualidade, fica reduzida à inserção em uma ou outra “categoria’’, como fruto da sua representação virtual a partir de dados coletados de modo autorizado ou não’’.

Segundo Laura Schertel Ferreira Mendes (2020, p. 14), “o direito à autodeterminação informativa, que garante o poder do indivíduo referente ao fornecimento e utilização dos seus dados pessoais, também age como norma de proteção, ou seja, como direito objetivo no âmbito privado [...]”. Dessa forma, é possível observar o consentimento como uma materialização da autodeterminação informativa, conforme definido no inciso XII do art. 5º da LGPD, que representa a “[...] manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada’’. Com efeito, a lei confere ao sujeito titular dos dados pessoais um protagonismo fundamental e inequívoco na proteção de suas informações (MENDES, 2020).

No julgamento do caso *Bundesverfassungsgericht* (1983), o Tribunal Constitucional Alemão decidiu, ao apreciar os limites dos poderes do Estado na coleta de dados para fins estatísticos, que a Autodeterminação Informativa – *Informationelles Selbstbestimmung* –, com fundamento na Dignidade da Pessoa Humana, é um elemento norteador do Direito à Proteção de Dados Pessoais (ROUVROY; POULLET, 2009; SILVA, 2012).

O reconhecimento da Proteção de Dados Pessoais como um Direito Constitucional garante uma posição privilegiada com relação a outras normas, porque se posiciona como um fenômeno cogente e garante uma aplicação supervisionada e validada pelo Tribunais Constitucionais, que avaliam a conformidade com princípios fundamentais (ROUVROY; POULLET, 2009).

Em continuação, a constitucionalização do direito à proteção de dados pessoais pode ser visualizada através de dois vetores: o do constitucionalismo formal e do constitucionalismo material (HERT; GUTWIRTH, 2009).

No constitucionalismo formal, analisa-se o processo de codificação da proteção de dados pessoais de forma expressa no rol de Direitos Fundamentais dos documentos Constitucionais (HERT; GUTWIRTH, 2009). Na Europa, esse processo é observado nas constituições nacionais, como a portuguesa, de 1976, que ao introduzir a figura do *Habeas Data*, consignou o direito ao conhecimento do processamento de dados pessoais, impondo restrições ao uso arbitrário de tais processamentos (HERT; GUTWIRTH, 2009). Além disso, a Constituição dos Países Baixos, com a revisão de 1983, atribuiu ao legislador a compertência de regular o uso das tecnologias de informação em prol da proteção da vida privada (HERT; GUTWIRTH, 2009). Outrossim, a Constituição Espanhola de 1978 reconheceu que o processamento de dados deveria ser restrito, com finalidade de garantir a honra e a privacidade (HERT; GUTWIRTH, 2009).

Dito isso, a formalização do Direito à Proteção de Dados Pessoais nos documentos constitucionais é uma reação aos percalcos enfrentados por uma sociedade gradualmente imersa na informação e comunicação (HERT; GUTWIRTH, 2009).

Há uma distinção das consituições entre codificadoras – ocupadas apenas em preservar principios tradicionais do Direito Constitucional – e transformadoras – que objetivam alterar a cultura constitucional (LESSIG, 1996; HERT; GUTWIRTH, 2009). Dessa forma, o movimento de constitucionalização do direito à proteção de dados pessoais, em seu vetor formal, traduz um movimento transformador (HERT; GUTWIRTH, 2009).

Esse movimento consagra constituições que promovem a proteção de dados com status de norma fundamental, tornando-as transformadoras, pois vão além do simples intuito de preservar valores constitucionais pressupostos e tradicionais, ao buscar adaptar as Constituições à realidade tecnológica contemporânea (LESSIG, 1996; HERT; GUTWIRTH, 2009). Assim, o constitucionalismo formal da proteção de dados pessoais não se limita a consignar Direitos Fundamentais, mas objetiva aproximar as constituições da realidade das práticas dataficadas da vida (HERT; GUTWIRTH, 2009).

Quanto ao Constitucionalismo Material, sua perspectiva, aplicada ao Direito à Proteção de Dados Pessoais, requer que os tribunais lutem pela concretização do direito à proteção de dados pessoais, de modo que as decisões não possuam uma cosmovisão apequenada do Direito à Proteção de Dados, limitando-o apenas a uma análise procedimental e indivualista (HERT; GUTWIRTH, 2009). Interpretações estritamente procedimentalistas do Direito à Proteção de Dados Pessoais criarão um ambiente digital inseguro, sujeito ao tráfico de informações pessoais, totalmente impune e imune (SILVA, 2012). Segundo Rengel (2013), o cumprimento da legalidade pode não oferecer proteção suficiente ao indivíduo e, pior, pode até contribuir para a violação de sua privacidade.

O julgamento das Ações Diretas de Inconstitucionalidade n. 6.387, 6.388, 6.389, 6.390 e 6.393, no âmbito do Supremo Trinunal Federal (STF), representa o principal marco no constitucionalismo material da proteção de dados pessoais, tendo impactado, segundo Pablo Trigo Kramcsák (2024), o entendimento sobre o compartilhamento de dados entre autoridades públicas. No referido julgado, consoante destacam Bruno Bioni et al. (2022, p. 11):

> […] decidiu-se pela inconstitucionalidade da Medida Provisória 954 de 2020 (…) que (…) previa o compartilhamento desproporcional de informações de operadoras de telefonia com o Instituto Brasileiro de Geografia e Estatística (IBGE), sem as necessárias salvaguardas e medidas que mitigassem os riscos aos titulares de dados pessoais.

Outro marco importante no constitucionalismo material da proteção de dados pessoais brasileira é a liminar proferida na ADI nº 6561/TO. Na referida ADI, discute-se o Cadastro Estadual de Usuários e Dependentes de Drogas criado pelo Estado do Tocantis (Brasil), através da Lei Estadual Lei nº 3.528/2019, de 12 de agosto de 2019. O Ministro Edson Fachin, relator da referida ADI no Supremo Tribunal Federal (STF), em seu voto, deferiu o pedido liminar de suspensão da eficácia da norma, argumentando que "[…] o cadastro tem um viés de seletividade e higienização social contrário aos direitos fundamentais insculpidos na CRFB/88, tais como a igualdade, a dignidade da pessoa humana, o direito à intimidade e à vida privada e o devido processo legal'' (MAGALHÃES; MATTIETTO, 2023, p. 165).

A partir de ambos os julgados, percebe-se como o Direito à proteção de dados pessoais é congulgado com outros elementos, como a proporcionalidade, nas ações Diretas de Inconstitucionalidade n. 6.387, 6.388, 6.389, 6.390 e 6.393, relatadas pela Ministra Rosa Weber (MENDES; RODRIGUES; FONSECA, 2023), e

a Dignidade da Pessoa Humana e o Direito à Privacidade, na ADI nº 6561/TO, relatada pelo Ministro Edson Fachin (MAGALHÃES; MATTIETTO, 2023).

A constitucionalização do Direito à Proteção de Dados Pessoais, para além de sua formalização nas constituições, envolve a interpretação das Cortes Constitucionais, buscando a melhor adequação de seus conceitos (BRKAN, 2022). Nesse sentido, a análise de Lessig (1996) e Hert e Gutwirth (2009) é relevante, pois, embora a proteção de dados pessoais, prevista no art. 5º da Constituição Federal pela introdução da Emenda Constitucional n. 115/2022, determine que a proteção de dados seja garantida “na forma da lei”, configurando o ápice do constitucionalismo formal da proteção de dados pessoais, é necessário observar que, quando a lei, por si só, não for suficiente para assegurar essa proteção, o julgador pode interpretar o direito a partir de outros Direitos Fundamentais previstos na Constituição.

Com base nas críticas de Hert e Gutwirth (2009) e Rengel (2013), o Direito à Proteção de Dados, com eficácia limitada, pode ser conjugado com o Direito à Privacidade, de eficácia plena, e com o Direito à Dignidade da Pessoa Humana. Uma interpretação mais ampla permite corrigir arbitrariedades da lei e garantir o constitucionalismo material da proteção de dados pessoais, reafirmando sua função constitucional transformadora.

É uma visão importante, pois a concepção individualista do direito à proteção de dados pessoais tem gerado distorções interpretativas sobre o fenômeno da constitucionalização do direito à proteção de dados pessoais (ROUVROY; POULLET, 2009). Ou seja, a individualização do direito à proteção de dados fez com que o direito se limitasse a uma pauta de satisfação, isto é, a proteção de dados se resumiria ao direito do sujeito de escolher entre manter as informações pessoais na esfera privada ou mercantilizá-las (ROUVROY; POULLET, 2009).

Isso porque a proteção de dados pessoais tem como núcleo a proteção da autonomia dos sujeitos, sendo algo diametralmente oposto à negociação comercial de informações pessoais (ROUVROY; POULLET, 2009). Essa crítica também é feita por Bart van der Sloot (2017b), ou seja, se a proteção de dados visa proteger o mercado, revestindo-se como um direito mercantil, é contraditório afirmar que se trata de um direito fundamental do sujeito, quando funciona como um direito fundamental do mercado. Rengel (2014) afirma que os direitos fundamentais não podem ser suprimidos por nenhuma autoridade e são inerentes à condição humana.

No caso *Bundesverfassungsgericht* (1983), quando o Tribunal Constitucional Alemão decidiu sobre o Direito à Proteção de Dados calcado na autodeterminação informativa, ficou inteligível que para que a autodeterminação informativa seja efetiva, é preciso que o sujeito não apenas detenha o poder de decisão, para além disso, é crucial que o sujeito tenha a capacidade real de implementar suas decisões sobre o uso e circulação de seus dados pessoais, sem pressão externa ou controle de terceiros (ROUVROY; POULLET, 2009; BIONI, 2016). Nesse ínterim, a autodeterminação informariva não deve ser apercebida como simples direito de negociar e comercializar dados pessoais, pois torna o Direito uma mercadoria, e o foco é mudado, ou seja, deixa de proteger a proteção da liberdade e da privacidade (ROUVROY; POULLET, 2009).

O destacado entrave dá-se à duas críticas que podem ser proferidas à Constitucionalização do Direito à Proteção de Dados Pessoais (ROUVROY; POULLET, 2009). Em primeiro lugar, a Proteção de Dados Pessoais, aconrada no consentimento do titular, abre margem para arbitrariedade que serão santificadas pela Lei (ROUVROY; POULLET, 2009; SILVA, 2012). Segundamente, com a introdução da Proteção de Dados Pessoais enquanto direito fundamental, tem-se sua equiparação com o Direito à Privacidade (ROUVROY; POULLET, 2009). Tal equiparação resulta na opacidade de valores fundamentais que sustentam tal proteção, como a Dignidade da Pessoa Humana e Autonomia dos Sujeitos (ROUVROY; POULLET, 2009). Assim, em que pese a constitucionalização do Direito à proteção de Dados pessoais, os valores mencionados precisam ser constantemente reafirmados como núcleo dessa proteção, ou seja, o Direito à Privacidade, à Dignidade da Pessoa Humana e a autonomia pessoal (ROUVROY; POULLET, 2009). Segundo Rouvroy e Poullet (2009), as implicações da constitucionalização do direito à proteção de dados pessoais pode ser corrigida, também, pela instituição de ações coletivas, a fim de equilibrar as assimetrias de poder entre titulares de dados e as grandes empresas.

Alvarez-Valenzuela (2020) argumenta que a constitucionalização do Direito à Proteção de Dados Pessoais forneceria uma proteção maior aos titulares. Contudo, no caso do Brasil, a constitucionalização do Direito à Proteção de Dados Pessoais transformou em eficácia limitada um direito que era de eficácia plena. A Constituição Federal de 1988 consagra em seu artigo 5º, X, o direito à intimidade, à vida privada,

à honra e à imagem, os quais devem ser respeitados e protegidos pelo Estado. Este direito, além de ser um direito fundamental, possui caráter de eficácia plena, significando que a proteção à privacidade não está sujeita a regulamentações que o possam mitigar de forma substancial. Trata-se de uma norma que possui eficácia plena, o que implica que seu alcance seja imediato, sem necessidade de tratamento infraconstitucional para sua aplicabilidade (SILVA, 1982; CARVALHO, 1998).

A Emenda Constitucional n. 115/2022, ao afirmar que o direito à proteção de dados pessoais é de eficácia limitada, adentra tal direito na Constituição contrariamente à natureza do direito à privacidade já consagrado como de eficácia plena (SILVA; NASCIMENTO; COSTA, 2023). A argumentação central dessa crítica reside no fato de que a Emenda reduz a abrangência da proteção constitucional, ao desconsiderar que a privacidade, em seu sentido pleno, é um direito fundamental com eficácia plena, conforme previsto no artigo 5º, inciso X, da Constituição Federal.

Portanto, a Emenda Constitucional nº 115/2022, ao submeter o direito à proteção de dados à regulamentação infraconstitucional e ao classificá-lo como de eficácia limitada, fere a natureza plena e imediata da privacidade, que é um direito fundamental de eficácia plena. Essa restrição não é compatível com a natureza de cláusula pétrea do Direito à Privacidade na Constituição, estando vedado qualquer emenda que implique em redução no que se refere à privacidade.

Apesar de tal crítica ser pertinente, é relevante destacar a perspectiva de Bruno Bioni e Fabricio Alves (2020, s/p.), que enaltece a natureza limitada da proteção de dados pessoais, conforme introduzida pela Emenda 115/2022. Segundo os autores, “[…] há elementos regulatórios da proteção de dados que necessitam de maior flexibilidade legislativa para concretização do próprio direito à autodeterminação informativa”.

Por fim, o direito à proteção de dados pessoais, ao ser constitucionalizado no Brasil, reflete um movimento transformador que visa adaptar o ordenamento jurídico à realidade tecnológica e às novas dinâmicas de poder informacional. Contudo, a limitação de sua eficácia pela Emenda Constitucional nº 115/2022 apresenta desafios significativos, pois contrapõe-se à natureza plena e imediata do direito à privacidade já consagrado como cláusula pétrea na Constituição Federal de 1988. Essa aparente tensão jurídica evidencia a necessidade de uma interpretação integrativa que harmonize a proteção de dados pessoais com os princípios

fundamentais da dignidade humana, da autonomia individual e da privacidade. Para isso, é indispensável que os tribunais desempenhem um papel ativo no fortalecimento do constitucionalismo material, garantindo que o direito à proteção de dados pessoais transcenda a esfera procedimental e reafirme seu caráter fundamental como um pilar ético e jurídico indispensável à construção de uma sociedade democrática.

2.3 O DIREITO À PROTEÇÃO DE DADOS PESSOAIS: A CRÍTICA DA AUTONOMIA

As preocupações da União Europeia em relação à proteção de dados pessoais têm levado à concepção de que tal direito teria fundamentalidade e, por consequência, autonomia jurídica (SARLET, 2021; TERWANGNE, 2022; RODOTÀ, 2009). Entretanto, a ideia de que o direito à proteção de dados pessoais deve ser considerado autônomo precisa ser revisada, pois não basta apenas considerá-lo como tal devido à sua formalização jurídica como um Direito Fundamental (SLOOT, 2017), como feito pela Carta de Direitos Fundamentais da União Europeia (2000) (RODOTÀ, 2009). Assim, igualmente, a ideia de que sua fundamentalidade melhora a proteção dos titulares (VERONESE et al., 2023a).

Rodotà (2009) destaca que o direito à proteção de dados não se subordina a outros direitos. No entanto, o grau de efetividade do direito à proteção de dados só pode ser medido pela satisfação do direito à privacidade. Se o cumprimento legal dos direitos de proteção de dados for insuficiente para garantir o direito à privacidade, ocorrerá uma violação deste direito, denominada por Rengel (2013) como “intervenção arbitrária à privacidade”. Rengel (2013) destaca o termo intervenções à privacidade, diferenciando entre intervenção ilegal e intervenção arbitrária. Nesse contexto, a intervenção ilegal é aquela que não respeita o postulado da legalidade, enquanto a intervenção arbitrária significa que, mesmo cumprindo a legalidade, a aplicação da lei ainda pode violar o objetivo e a finalidade do direito à privacidade, o que exige a aplicação do princípio da razoabilidade na interpretação desse direito (RENGEL, 2013).

Portanto, se a efetividade do direito à proteção de dados é sempre analisada em última instância pela satisfação do direito à privacidade, Rodotà (2009) comete um equívoco ao afirmar que ele é um direito insubordinado aos demais. O citado

equívoco é reconhecido, ainda que de forma não intencional, pelo próprio Rodotà (2009), quando ele menciona a necessidade de realizar estudos de impacto sobre o direito à privacidade, semelhante ao que é feito no direito ambiental, para garantir um nível satisfatório de proteção de dados pessoais. Ao propor tal medida, Rodotà (2009) implicitamente reconhece que o direito à proteção de dados é subordinado ao direito à privacidade.

A vertente procedimental do direito à privacidade, conforme descrito por Anderson Schreiber (2014), demonstra como o direito à proteção de dados serve como uma ponte para a consecução da vertente substancial do direito à privacidade. A partir do texto de Maria Tzanou (2013), pode-se afirmar que o direito à proteção de dados possui normas próprias, objeto específico, reconhecimento social e jurídico, e sanções específicas. Entretanto, o direito à proteção de dados não possui autonomia em relação ao direito à privacidade, pois a ausência deste último prejudica a identidade e, principalmente, a aplicabilidade da proteção de dados pessoais.

Maria Tzanou (2013) descreve que nem todo dado pessoal é, por si só, ofensivo ao direito à privacidade, o que poderia sugerir uma distinção clara entre o direito à proteção de dados pessoais e o direito à privacidade. De fato, ao analisar informações como nome, e-mail ou número de matrícula de veículo isoladamente, esses dados podem não parecer prejudiciais à vida privada. No entanto, a combinação dessas informações com outros dados pode gerar danos à privacidade do titular, como no caso de práticas de *phishing* através do simples vazamento de um e-mail. Ou seja, mesmo que um dado seja considerado inofensivo à primeira vista, ele pode ser utilizado posteriormente para finalidades que ofendam a privacidade de forma significativa.

Por essa razão, a legislação antecipa tais situações, regulando até mesmo os dados aparentemente inofensivos, para evitar qualquer situação prejudicial e, assim, prevenir a violação da privacidade. Dessa forma, a proteção de dados pessoais, ainda que inicialmente pareça distinta do direito à privacidade, está intrinsecamente ligada a ele, pois visa impedir que a privacidade seja comprometida, mesmo em situações onde o risco não é imediatamente evidente.

Segundo Tzanou (2013), é possível afirmar o direito à proteção de dados como uma liberdade afirmativa, que não visa proibir o poder, mas sim garantir a liberdade de ação (TZANOU, 2013; BIONI; ALVES, 2020; BIONI, 2014). No entanto,

o direito à proteção de dados, como liberdade afirmativa, é menos fundamental do que as liberdades negativas, como a privacidade, que protegem contra intromissões externas (TZANOU, 2013). Por depender de ações positivas para sua efetivação, ele acaba vinculado à privacidade, que serve como base essencial para sua justificativa e aplicação. Assim, a tentativa de autonomia do direito à proteção de dados revela sua dependência em relação à privacidade, reforçando que ambos estão intrinsecamente conectados.

Maria Tzanou (2013) destaca que, para conceber o direito à proteção de dados como um direito fundamental e autônomo, é necessário que ele consiga operar tanto de maneira negativa quanto positiva, ou seja, que consiga, ao mesmo tempo, afastar o poder e controlá-lo. A autora sugere que o direito à proteção de dados pessoais possui um “núcleo duro” que o consagra como um direito independente, pois resguarda a autonomia individual, a identidade e a dignidade da pessoa humana.

Entretanto, Tzanou (2013) não fundamenta por que esses valores não poderiam ser albergados pelo direito à privacidade. Considerando a evolução jurisprudencial norte-americana e do Tribunal Europeu de Direitos Humanos, destacada na seção 2.1, o direito à privacidade sempre se mostrou eficaz em assegurar tais mandamentos. Se o direito à privacidade já exerce essa função, seria redundante afirmar que o direito à proteção de dados pessoais é autônomo simplesmente porque exerce as mesmas funções.

É possível avaliar o direito à proteção de dados sob a lente da proporcionalidade sem uma referência direta ao direito à privacidade, como Maria Tzanou (2013) sugere. No entanto, isso levanta questões filosóficas fundamentais: qual é o critério que permite julgar algo como desproporcional? Ao afirmar que uma informação é injusta, em que basear essa injustiça? A resposta reside na natureza subjacente do direito à privacidade, que serve como uma régua ética inescapável. A desproporcionalidade na proteção de dados surge precisamente porque há uma transgressão à privacidade, e uma informação se torna injusta na medida em que a violação à privacidade se revela intrinsecamente iníqua. Portanto, mesmo ao aplicar a proporcionalidade, o direito à privacidade permanece como o fundamento ético e jurídico essencial para julgar a adequação e a justiça na proteção de dados pessoais.

A interpretação jurídica, segundo Dworkin (1989), deve buscar a melhor luz para resolver conflitos entre direitos, levando em conta sua coerência com o todo do sistema jurídico. Aplicado ao contexto da proteção de dados, isso implica que a proporcionalidade não é apenas uma ferramenta técnica, mas um processo que reflete os valores fundamentais da privacidade. Quando o direito à proteção de dados não garante plenamente a privacidade, ele não está cumprindo seu papel como direito intermediário, reforçando sua subordinação ao direito à privacidade.

O julgador pode, de fato, recorrer ao critério da desproporcionalidade para invalidar uma violação do direito à proteção de dados pessoais sem necessariamente invocar o direito à privacidade. No entanto, como o brilho do sol não mudaria se o chamassem de lua, a influência do direito à privacidade na ordem dos direitos fundamentais é inevitável (RENGEL, 2013). Mesmo que de forma subjacente, o direito à privacidade continua a subjugar o direito à proteção de dados, servindo como a base ética e jurídica que orienta e fundamenta a proteção de dados pessoais. A privacidade, portanto, permanece como a essência que ilumina e justifica a validade das normas e julgamentos relacionados à proteção de dados.

O fato de o direito à proteção de dados estar sendo formalizado como direito fundamental em vários países, inclusive no Brasil, não esclarece como esse direito seria independente em relação ao direito à privacidade. Discutir a autodeterminação informativa como uma distinção para a aplicação da proteção de dados pessoais parece equivocado, especialmente por ignorar que, na evolução do direito à privacidade, a autonomia da vontade — em uma acepção muito similar à autodeterminação informativa — foi preservada e caracterizada, ainda que de maneira rudimentar, como um instituto sagrado do direito à privacidade. Um exemplo disso é o caso em que o tribunal francês, em 1900, decidiu sobre a necessidade de coleta do consentimento da pessoa retratada em uma pintura para a exposição pública do retrato (WEEKS, 1963).

Essa continuidade histórica demonstra que a autodeterminação informativa não é uma inovação exclusiva do direito à proteção de dados, mas uma característica fundamental da privacidade. Portanto, afirmar a independência do direito à proteção de dados com base na autodeterminação informativa desconsidera o fato de que essa mesma autonomia já faz parte do direito à privacidade há muito tempo.

Ingo Sarlet (2021) acerta ao afirmar que o direito à proteção de dados não se confunde com o direito à privacidade, mas se equivoca quanto às suas motivações. Da mesma maneira, o sigilo de correspondência não se confunde com o direito à privacidade. Um direito específico nunca será confundido com um direito mais amplo, pois não terá o mesmo alcance (KUNER, 2009b).

O argumento de Ingo Sarlet (2021) seria suficiente para afirmar a autonomia do sigilo de correspondência, porque este não se confunde com o direito à privacidade. A abrangência e a profundidade do direito à privacidade acabam por englobar e sobrepor esses direitos específicos, questionando a necessidade de considerá-los autônomos quando, na verdade, eles funcionam como componentes ou extensões do direito à privacidade.

O conceito de privacidade é bastante diverso (MOORE, 2008; KUNER, 2010c), o que resulta na formação de direitos distintos que compõem um conjunto de direitos intermediários (ROUVROY; POULLET, 2009). Assim, o conceito geral de direito à privacidade será sempre mais amplo do que o conceito atribuído a qualquer direito intermediário (ROUVROY; POULLET, 2009; KUNER, 2009b).

As menções feitas por Ingo Sarlet (2021) ao direito à proteção de dados como autônomo em relação à privacidade deixam de abordar uma questão crucial: por que o direito à privacidade teria perdido sua autonomia? Segundo Sloot (2017b) e Veronese et al. (2023a), a aparente incapacidade do direito à privacidade em lidar com a dimensão informativa da sociedade contemporânea levou ao fortalecimento do direito à proteção de dados pessoais, sem considerar a possibilidade de uma dimensão coletiva do direito à privacidade. No entanto, conforme as considerações de Bart van der Sloot (2017b), o direito à proteção de dados, ao tentar superar as supostas deficiências do direito à privacidade, acabou por reproduzir os mesmos institutos e, com isso, replicou a mesma ineficiência que motivou sua origem como um direito, destacados por Bart van Der Sloot (2017b) a partir da deficiência das doutrinas *ratione personae* e *ratione materiae* para lidar com o *big data*.

Sarlet (2021) afirma que, ao abranger todos os dados de uma pessoa natural, o direito à proteção de dados é mais abrangente do que o direito à privacidade. Contudo, essa afirmação parte de uma premissa otimista de que o direito à proteção de dados é presumidamente infalível. Mas, quando a observância das disposições legais relativas ao direito à proteção de dados não for suficiente para resguardar a

liberdade do sujeito, qual será o recurso do intérprete para julgar a arbitrariedade? Rengel (2013) expõe que o direito à privacidade pode ser violado pela arbitrariedade da lei, e que, dependendo do caso concreto, o cumprimento estrito da legalidade pode não ser suficiente para garantir a proteção adequada.

Como discutido anteriormente com base em Rengel (2013) e nas deduções feitas a partir do texto de Tzanou (2013), as falhas do direito à proteção de dados serão inevitavelmente submetidas ao direito à privacidade, revelando sua dependência. Assim, o direito à privacidade atua como instância final para resolver as lacunas e arbitrariedades que o direito à proteção de dados, por si só, não consegue solucionar. Isso reafirma a posição do direito à privacidade como o alicerce fundamental.

Bart van der Sloot (2017) destaca que, se a principal preocupação da proteção de dados é a proteção da privacidade, não há necessidade de concebê-la como um direito fundamental, uma vez que tal proteção já estaria amparada na tradição do direito à privacidade e nas declarações de direitos humanos.

No entanto, se for argumentado que a idiossincrasia da proteção de dados reside na necessidade de manter incólumes os fluxos de dados para a fruição da economia digital, Sloot (2017) aponta que seria igualmente estranho considerar um direito mercantil—que não coloca o sujeito como centro de proteção, mas sim o fluxo de dados para a economia—como um direito fundamental.

Ademais, Sloot (2017b) destaca que é problemático considerar a proteção de dados um direito fundamental porque mesmo dados simplórios, como o nome de uma pessoa, seriam considerados parte do direito fundamental à proteção de dados pessoais, o que se distingue significativamente das tradicionais declarações de direitos humanos e de direitos fundamentais, que consideram graves violações de direitos e não quaisquer violações, até mesmo as mais simples. Nesse contexto, Sloot (2017b) argumenta que a proteção de dados é, na verdade, um direito comum e não um direito fundamental, pois lhe falta o caráter essencial de fundamentalidade.

Essa discussão é relevante, pois a visão fundamentalista da “fundamentalização” do direito à proteção de dados implicaria que não haveria diferença significativa entre a violação de um direito fundamental e a violação de um direito comum. Como resultado, a violação dos direitos fundamentais poderia se tornar algo cotidiano, naturalizando-se (SLOOT, 2017a). Isso, por sua vez, poderia

enfraquecer a gravidade e a excepcionalidade que devem ser associadas à violação de direitos verdadeiramente fundamentais.

A afirmativa de Sloot (2017a) contém uma crítica jurídica fundamental. Ou seja, ao tratar a proteção de dados como um direito fundamental, pode-se tornar impossível distinguir entre regras e casos que envolvem direitos verdadeiramente fundamentais e aqueles que não o fazem. Isso pode impedir que decisões sejam tomadas de forma justa e adequada, comprometendo a clareza e a eficácia da aplicação dos direitos fundamentais (SLOOT, 2017a).

A discussão sobre a “fundamentalização” do direito à proteção de dados também está intimamente ligada à crítica dworkiniana à fragmentação de princípios fundamentais. Dworkin (1986; 1985) argumenta que a fragmentação de princípios enfraquece a integridade do sistema jurídico, criando direitos que competem entre si em vez de se reforçarem mutuamente. No caso da proteção de dados, tentar desvinculá-lo da privacidade compromete sua coesão e justificativa moral. Isso é evidente na medida em que a proteção de dados, como apontado acima, é incapaz de operar de forma totalmente independente, pois precisa recorrer à privacidade para justificar suas normas e aplicações.

Bart van der Sloot (2017b) identifica que, hodiernamente, o direito à proteção de dados tem sido associado ao livre desenvolvimento da personalidade. Tal justificativa parece mais lógica do que conferir um status de direito autônomo e fundamental ao direito à proteção de dados pessoais. Isso porque, conforme afirma Bart van der Sloot (2017), o direito ao livre desenvolvimento da personalidade abrange tanto a proteção na ocultação quanto na publicação de aspectos inerentes à vida do sujeito. Portanto, o aparente afastamento do direito à proteção de dados pessoais em relação ao direito à privacidade não o posiciona para uma autonomia, mas sim, talvez, para uma mudança de dependência para o livre desenvolvimento da personalidade.

Foi sob o manto do livre desenvolvimento da personalidade, segundo Sloot (2017b), que se iniciou a adequação e ponderação de interesses na aplicação negativa do direito à privacidade. Ou seja, os aspectos positivos do livre desenvolvimento da personalidade tornam-se igualmente relevantes (SLOOT, 2017b). A proteção de dados não lida apenas com dados privados; mesmo quando o dado é exposto, a autorrevelação do sujeito continua a ser protegida pelo livre

desenvolvimento da personalidade (SLOOT, 2017b). Portanto, mesmo que um dado pessoal esteja marcado com a dispensa da coleta do consentimento, considerando os interesses do agente de tratamento, ainda assim é exigido o devido tratamento dos dados pessoais (SLOOT, 2017b), pois atributos da personalidade do sujeito estão sendo manuseados.

In fine, o direito à proteção de dados pessoais, embora tenha ganhado destaque como um direito fundamental em muitos ordenamentos jurídicos, incluindo o Brasil, ainda enfrenta desafios conceituais e práticos quanto à sua autonomia em relação ao direito à privacidade. A análise revela que sua justificativa e aplicação continuam intrinsecamente ligadas à privacidade, seja como fundamento ético, seja como parâmetro de proteção contra arbitrariedades legais. A tentativa de "fundamentalizar" o direito à proteção de dados como um direito autônomo pode levar a uma fragmentação perigosa dos princípios fundamentais, conforme critica Dworkin (1986), e comprometer sua eficácia ao dissociá-lo de valores essenciais como a dignidade e a liberdade. Ademais, a relação entre a proteção de dados e o livre desenvolvimento da personalidade oferece uma perspectiva mais ampla e dinâmica, reconhecendo a importância tanto da ocultação quanto da autorrevelação. Assim, embora o direito à proteção de dados desempenhe um papel crucial na contemporaneidade, sua efetividade e justificativa dependem de sua integração harmoniosa com outros direitos fundamentais, especialmente o direito à privacidade, evitando a superficialidade de uma autonomia meramente formal.

3 A TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS: DIÁLOGOS JURÍDICOS E TENSÕES NO CENÁRIO GLOBAL

3.1 TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS: UM PROBLEMA JURISDICIONAL

O embrião da proteção de dados pessoais, surgido no Estado de Hessen, Alemanha, em 1970, não previa disposições específicas sobre a transferência internacional de dados (KUNER, 2010c). Logo depois, diversos países europeus, como Finlândia, Irlanda, Áustria, França, Suécia e Luxemburgo, regularam a proteção de dados pessoais impondo restrições à transferência internacional de dados (KUNER, 2010c). Essas restrições tinham como objetivo evitar que informações fossem enviadas para nações com regulações insuficientes para

garantir uma proteção adequada (KUNER, 2010c). De forma mais específica, tais medidas incluíam a exigência de autorização prévia de autoridades competentes, a adoção de normas alinhadas à Convenção 108 do Conselho da Europa e a obrigatoriedade de consentimento ou de mecanismos que garantissem uma proteção equivalente (KUNER, 2010c). Apesar de a preocupação desses países ser pertinente à época, a transferência de dados pessoais era vista como um evento pontual e não como algo tão disseminado e central quanto é na atualidade (KUNER, 2010c; ALBORNOZ, 2022).

Com a intensificação das transferências internacionais de dados, surgiu uma significativa insegurança em relação à aplicação das leis de privacidade, pelo descontrole informacional gerado pelo volúme dos fluxos internacionais de dados (KUNER, 2009a; KUNER, 2010a; KUNER, 2010c; RAMIRO, 2022; KUNER, 2020a; TERWANGNE, 2009). Com a virtualização da globalização e o deslocamento das relações internacionais para o ambiente digital, essas interações passaram a estar sujeitas a jurisdições distintas e cada vez mais complexas (KUNER, 2009a; KUNER, 2010a; KUNER, 2017; SUDA, 2017; KUNER, 2020a; RYNGAERT; TAYLOR, 2020; BIONI, 2014). Entre 2005 e 2014, as transferências internacionais de dados aumentaram 45 vezes em escala global, um crescimento impulsionado pela expansão das tecnologias em nuvem (SUDA, 2017).

A mencionada preocupação levou a sociedade internacional a demonstrar um interesse crescente na regulação das transferências internacionais de dados pessoais (KUNER, 2020a; TERWANGNE, 2009), especialmente após eventos críticos, como as revelações de Edward Snowden em 2013 (KUNER, 2014; KUNER, 2021; KUNER et al., 2015; KUNER et al., 2016; CHIAPPETTA, 2018). As revelações impulsionaram debates sobre a expansão da vigilância nas relações internacionais (KUNER et al., 2013; KUNER, 2020e; COCHE; KOLK; OCELÍK, 2024; CHIAPPETTA, 2018). À medida que os dados pessoais passaram a ser considerados um ativo financeiro fundamental na economia digitalizada (KUNER, 2010c; BOSHE, 2015), também ganharam projeção como um elemento essencial de soberania (ANDREWS, 2020; BELLI et al., 2024; KUNER et al., 2015).

Apesar da quantidade surpreendente de transferências internacionais de dados, que são a força motriz da nova economia global sob uma lógica de vigilância (ZUBOFF, 2021; ZUBOFF, 2015; CHIAPPETTA, 2018), essas operações não

recebem a devida atenção no campo jurídico (KUNER et al., 2013; KUNER, 2010c). De forma geral, os países têm priorizado, em primeiro plano, a regulação interna da proteção de dados, relegando a regulação das transferências internacionais a um segundo plano (KUNER, 2010c).

No caso do Brasil, a regulamentação do tratamento de dados para agentes de tratamento de pequeno porte, estabelecida na Resolução n.º 02/2022, sendo a segunda publicação da ANPD, foi implementada antes do Regulamento de Transferência Internacional de Dados, aprovado pela Resolução n.º 19/2024. Ou seja, evidencia-se uma falta de prioridade na regulamentação das transferências internacionais de dados, uma vez que questões voltadas a agentes de pequeno porte foram normatizadas previamente, enquanto um tema de maior impacto global e estratégico, que envolve o fluxo transfronteiriço de informações e a adequação do Brasil aos padrões internacionais de proteção de dados, permaneceu sem regulamentação específica por um período mais prolongado.

Nesse contexto, percebe-se que as regulações de proteção de dados frequentemente são vistas como obstáculos ao livre comércio (CELLI, 2020). Dessa forma, quanto menores forem as barreiras relacionadas aos dados, mais eficientes tendem a ser as transações comerciais (SUDA, 2017). Diante dessa realidade, países com regulações mais frágeis em matéria de privacidade têm sido denominados “paraísos de dados” (ANGARITA; ZULUAGA, 2019; SUDA, 2017).

Nessa senda, as transferências internacionais de dados podem ser categorizadas como abertas, condicionadas ou limitadas (COCHE; KOLK; OCELÍK, 2024). Na transferência aberta, as empresas não têm obrigações específicas relacionadas às transferências internacionais e podem agir de forma livre (COCHE; KOLK; OCELÍK, 2024). Na transferência condicionada, esta deve ocorrer conforme as hipóteses estabelecidas pela legislação, ou seja, as empresas estão vinculadas à lei (COCHE; KOLK; OCELÍK, 2024). Já na transferência limitada, a realização depende de autorização do governo exportador ou importador, ou é simplesmente proibida (COCHE; KOLK; OCELÍK, 2024).

Com o advento da internet, Svantesson (2017) divide a história da jurisdição no fluxo internacional de dados pessoais em cinco fases. Inicialmente, não existia qualquer regulação, já que o surgimento da internet, em um primeiro momento, não implicou grandes transferências de informações entre diferentes jurisdições

(SVANTESSON, 2017). Svantesson (2017) descreve essa primeira fase como período pré-1991.

A segunda fase, delimitada por Svantesson (2017) entre 1991 e 1999, ocorreu com o surgimento da *World Wide Web (WWW)*. Nesse período, a internet foi considerada uma *terra nullius*, um espaço ainda sem regulamentação definida, caracterizado pela percepção de um ciberespaço onde não se vislumbravam fronteiras ou limites jurisdicionais claros (SVANTESSON; 2017; OLDANI, 2020).

Entre os anos de 2000 e 2009, Svantesson (2017) identifica o surgimento da terceira fase, marcada pela chamada fase da regulação excessiva. Nesse período, tribunais e legisladores adotaram posturas mais extremas em relação à aplicação extraterritorial das leis, estendendo a aplicação de normas nacionais a conflitos que afetavam cidadãos em outras jurisdições. Dois casos emblemáticos ilustram essa fase: o caso *Gutnik*, na Austrália, e o caso *Yahoo!*, na França (SVANTESSON, 2017). Nesse contexto, Suda (2017) define a extraterritorialidade como a aplicação de normas e legislações internas a agentes externos e suas atividades, independentemente do território de onde essas ações se originam ou se desenvolvem.

A quarta fase descrita por Svantesson (2017), compreendida entre 2010 e 2014, é denominada como a fase da sub-regulamentação, que é caracterizada por abordagens inconsistentes para lidar com os desafios relacionados à jurisdição e à internet (SVANTESSON, 2017). Nesse período, observou-se um aumento tanto nas medidas legais adotadas pelos Estados quanto na intensificação dos estudos acadêmicos sobre o tema, refletindo esforços para compreender e enfrentar as complexidades dessa nova realidade jurídica (SVANTESSON, 2017).

Svantesson (2017) propõe uma quinta fase, a mais recente, iniciada a partir de 2015, que ele denomina como a “era da hiper-regulamentação”, marcada pelo encurtamento das relações entre jurisdições por meio da internet, o que traz à tona problemas legais cada vez mais complexos e exige uma regulação mais detalhada e abrangente para lidar com a crescente interconexão global.

Após o contexto histórico delineado por Svantesson (2017), trazendo o debate para a contemporaneidade, observa-se que os fluxos transfronteiriços de dados pessoais geram enormes incertezas (KUNER, 2009a; KUNER, 2014). Essas incertezas submetem empresas a custos de transação instáveis e colocam os

indivíduos em uma posição de obscuridade quanto à destinação e ao tratamento de seus dados (KUNER, 2009a; KUNER, 2014). Nesse sentido, Svantesson (2017) apresenta uma afirmação contundente ao enfatizar que todos os agentes envolvidos na transferência internacional de dados precisam recorrer ao Direito. Os usuários não desejam uma internet que não seja segura, e o comércio internacional depende de uma internet regulada de forma previsível (SVANTESSON, 2017). Assim, deixar de regular os fluxos transfronteiriços de dados não é uma alternativa viável (SVANTESSON, 2017). Para abordar essa questão, Kuner (2009a) estabelece um *a priori* centrado na problemática jurídica da jurisdição, que se mostra cada vez mais desafiada no cenário atual (SVANTESSON, 2017).

Na doutrina contemporânea do direito internacional, a jurisdição é comumente classificada em três categorias: (I) prescritiva, (II) adjudicativa e (III) de execução (KUNER, 2010a; KUNER, 2010b; SVANTESSON, 2017; SVANTESSON, 2016; OLDANI, 2020). A classificação surge como uma forma de compreender a jurisdição em sua dimensão exorbitante e é reconhecida pela Comissão de Direito Internacional da ONU (KUNER, 2010b).

No entanto, Svantesson (2017) ressalta que tal categorização não é rígida ou exaustiva, alertando que não deve ser vista como a única maneira de conceituar a jurisdição. Além disso, o autor destaca a ausência de consenso sobre os papéis e os limites de cada uma dessas categorias, o que reforça a necessidade de uma abordagem mais flexível e contextualizada para o entendimento da jurisdição no direito internacional.

Na jurisdição prescritiva, observa-se o poder de um Estado de criar e aplicar suas legislações em situações que envolvam agentes estrangeiros, como pessoas, bens ou dados, mesmo que estejam localizados fora de seu território (KUNER, 2010a; SVANTESSON, 2016; OLDANI, 2020).

Na jurisdição adjudicativa, concebe-se a possibilidade de tribunais julgarem casos que envolvam agentes estrangeiros (KUNER, 2010a; SVANTESSON, 2016; OLDANI, 2020). Nesse contexto, a publicização do direito à proteção de dados pessoais reúne as funções jurisdicionais adjudicativa e prescritiva (KUNER, 2010a). Um fenômeno que reforça, por meio do novo paradigma de jurisdição baseado no princípio da personalidade (KUNER, 2009a), a soberania estatal, mesmo diante de

um ambiente jurídico internacional marcado por sua extrema complexidade e interconexão.

A jurisdição no aspecto de execução refere-se ao poder de um Estado em realizar atos no território de outro Estado (KUNER, 2010a; SVANTESSON, 2016; OLDANI, 2020). Assim, a questão não se limita apenas à classificação da jurisdição, mas envolve a compreensão de seus limites, especialmente considerando que o sistema internacional de direito público é notoriamente frágil nesse aspecto (KUNER, 2010a).

Ainda há a figura da *Effects Doctrine* (doutrina dos efeitos), amplamente discutida como princípio norteador da jurisdição (KUNER, 2010a). Para a teoria mencionada, ações que causam violações à proteção de dados de cidadãos localizados no Brasil podem atrair a jurisdição brasileira, mesmo que estejam submetidas a outras jurisdições. Todavia, a concepção é alvo de críticas significativas, especialmente por sua falta de limites claros (KUNER, 2010a). Em um ambiente globalizado, onde as causalidades se entrelaçam de maneira constante, argumenta-se que, sob essa lógica, tudo poderia causar efeito em tudo, o que gera incertezas e inseguranças jurídicas (KUNER, 2010a).

A jurisdição, tradicionalmente vinculada ao princípio da territorialidade (KUNER, 2010a; KUNER, 2010c), estabelece que cada jurisdição corresponde a um território, e os acontecimentos dentro desse espaço estão sujeitos à legislação local. Contudo, os novos modelos de negócios têm progressivamente desvalorizado o critério geográfico (KUNER, 2010c). Além disso, o princípio da territorialidade se mostra inadequado no contexto da internet (KUNER, 2010c), o que é reforçado por Leighton Andrews (2020), Bruno Bioni (2014) e Oldani (2020), ao argumentarem que a internet, enquanto ambiente sem fronteiras, desafia o conceito tradicional de Estado-nação, assim como os fundamentos de soberania e jurisdição que dependem de delimitações territoriais para sua operacionalização.

A ausência de fronteiras no ciberespaço pode levar à concepção de que se trata de um ambiente *res communes omnium*, ou seja, um bem comum global (OLDANI, 2020). Todavia, embora possa ser entendido dessa forma (OLDANI, 2020), há proprietários que exercem controle sobre sua estrutura e funcionamento (ANDREWS, 2020). Dessa maneira, configura-se como um espaço simultaneamente público e privado (RENGEL, 2014). Justamente por isso, Niels van Doorn (2020) e

Reginaldo Felix Nascimento e Lucas Gonçalves da Silva (2024) analisam o citado fenômeno como uma dinâmica que desafia os limites entre o público e o privado, mas que, antes de qualquer aspecto, deve ser reconhecido como uma nova instituição na sociedade.

Segundo Oldani (2020), a soberania, definida pelo princípio da territorialidade, orienta as relações internacionais e fundamenta a independência entre os Estados. É a partir do conceito de soberania que os Estados podem invocar o poder estatal para controlar os objetos, pessoas e bens tutelados dentro de seus territórios, poder que é determinado pela perspectiva da jurisdição (OLDANI, 2020). Assim, soberania e jurisdição são simbióticas, uma vez que a jurisdição representa a autoridade para prescrever, executar e julgar (OLDANI, 2020), conforme acima descrito.

Com o aparente declínio do princípio da territorialidade (BIONI, 2014), ganha destaque a aplicação da jurisdição baseada no princípio da personalidade, que se divide em personalidade ativa e passiva (KUNER, 2010a). Nesse cenário, a jurisdição passa a ser definida por um critério *ratione personae,* desvinculado do território. Na prática, tal afirmação indica que a jurisdição é aplicada com base na nacionalidade do sujeito ativo ou passivo (KUNER, 2010a). Assim, no caso da vítima, prevalecem as leis de sua nacionalidade, fundamentadas no princípio da personalidade passiva (KUNER, 2010a). Da mesma forma, em relação ao sujeito que comete a violação de dados pessoais, aplica-se a jurisdição com base no princípio da personalidade ativa (KUNER, 2010a).

Nessa linha de debates, destaca-se ainda o princípio da proteção (KUNER, 2010a). De acordo com esse princípio, um Estado soberano pode realizar ações em outros países, desde que essas medidas sejam voltadas à defesa de sua soberania contra ameaças externas (KUNER, 2010a). Contudo, no âmbito da proteção de dados, Kuner (2010a) observa que esse princípio possui pouca relevância para a defesa de interesses individuais, sendo mais aplicável a questões relacionadas à proteção de interesses estatais.

De forma geral, a jurisdição surge com a missão de apaziguar conflitos entre sociedades, fundamentando-se inicialmente na já mencionada ideia de personalidade. Tal concepção vinculava a jurisdição a fatores como a nação, religião,

grupo étnico ou tribo a que um sujeito pertencia, caracterizando-se como um modelo pré-territorial (KUNER, 2009a; SVANTESSON, 2017).

Com o Tratado de Vestfália de 1648, Kuner (2009a) destaca que o princípio da personalidade perdeu força, devido ao privilégio assumido pelo princípio da territorialidade na determinação das jurisdições.

Atualmente, a proteção de dados é vista a partir da perspectiva da jurisdição baseada na personalidade, considerando que o ciberespaço, ao se apresentar como um ambiente sem fronteiras, desafia o princípio da territorialidade que fundamenta a concepção de soberania no Estado-nação contemporâneo (RYNGAERT; TAYLOR, 2020; KUNER, 2009a; ANDREWS, 2020). Nesse sentido, Kuner (2009a) aponta para um retorno ao conceito de jurisdição baseada na personalidade, considerando o enfraquecimento da territorialidade nas relações contemporâneas.

Kuner (2010b) considera que as preocupações relacionadas à jurisdição e à internet são frequentemente exageradas. Ele argumenta que as afirmações unilaterais de jurisdição promovidas por Estados na internet seguem padrões semelhantes aos observados em outros contextos. Além disso, a geolocalização permite uma jurisdição baseada no princípio da territorialidade, o que ajuda a minimizar conflitos decorrentes da sobreposição de múltiplas jurisdições (*overlapping*) ou da aplicação desproporcional de uma jurisdição sobre outra (*exorbitant*). Kuner (2010b) também observa que a regulação preocupa apenas os países que possuem capacidade efetiva de executar medidas, e que o comércio internacional sempre enfrentou custos e instabilidades resultantes das diferentes jurisdições.

Ao abordar a jurisdição na transferência internacional de dados, Svantesson (2017) destaca a geolocalização como um instrumento tecnológico de destaque para operacionalizar o princípio da territorialidade da jurisdição. Contudo, essa tecnologia apresenta falhas de precisão, o que compromete a aplicação de um princípio digital da territorialidade igualmente impreciso (SVANTESSON, 2017), especialmente considerando que tecnologias de geolocalização podem ser facilmente contornadas (SVANTESSON, 2017), como no caso do uso de VPNs . Ainda assim, Svantesson (2017) argumenta que a geolocalização é fundamental para aproximar a internet do mundo real, estruturando-a em divisões territoriais com fronteiras claras e submetidas a diferentes sistemas legais.

Kuner (2009a) afirma que a regulação das transferências internacionais de dados está profundamente vinculada à natureza essencialmente pessoal dos dados. Além disso, a Diretiva da União Europeia desconsidera o conceito de territorialidade ao tratar da regulação dessas transferências, optando por adotar o conceito de jurisdição baseado na personalidade como fundamento central (KUNER, 2009a).

Em outras palavras, ao determinar que os dados devem ser transferidos apenas para jurisdições que a União Europeia considere como possuindo níveis de proteção adequados, a União Europeia transmite, de forma implícita e intersubjetiva, a mensagem de que seus dados estarão acompanhados por suas legislações e padrões éticos, independentemente do local para onde sejam enviados (KUNER, 2009a; KUNER, 2021).

A personalização da jurisdição está refletida nos princípios de privacidade da APEC (*Asia-Pacific Economic Cooperation*) (KUNER, 2009a; KUNER, 2010a). Nesse contexto, o princípio da personalidade, na concepção da APEC, manifesta-se através do conceito de *accountability* em privacidade, que estabelece a responsabilidade do agente de tratamento de dados em proteger os dados conforme o padrão original de privacidade, ou seja, respeitando a legislação de privacidade vigente no local e no momento da coleta (KUNER, 2009a; KUNER, 2010a). O compromisso permanece válido independentemente das jurisdições posteriores em que os dados sejam processados ou armazenados (KUNER, 2009a). Em outras palavras, a legislação aplicável ao titular dos dados “acompanha” o dado, onde quer que ele esteja (KUNER, 2021).

As críticas à agressividade das regulamentações de dados da União Europeia não impediram a expansão da jurisdição baseada na personalidade (KUNER, 2009a). O GDPR, por exemplo, amplia significativamente o escopo territorial de sua aplicação (PRAMESTI; AFRIANSYAH, 2020; ALBORNOZ, 2022). Tal expansão levanta questões complexas para o Direito Internacional, pois a convivência entre uma jurisdição fundamentada na personalidade e uma cultura jurídica ainda predominantemente territorial gerou inúmeros conflitos relacionados à extraterritorialidade das leis de privacidade (KUNER, 2009a; KUNER, 2010a; KUNER, 2010b; KUNER, 2017). Embora os Estados possam legislar de forma a conferir alcance extraterritorial às suas normas (KUNER, 2009a; SVANTESSON, 2013; SVANTESSON, 2015), o direito internacional exige que a aplicação dessas

normas em outros países dependa da permissão explícita das respectivas jurisdições territoriais (KUNER, 2009a).

O princípio da personalidade foi reafirmado no caso C-131/12, julgado em 13 de maio de 2014, envolvendo o Google Espanha, a AEPD (Agência Espanhola de Proteção de Dados) e Mario Costeja González (KUNER, 2014; KUNER, 2017). Nesse caso, que abordava o processamento de dados por um agente de tratamento localizado fora da jurisdição da União Europeia, o Tribunal de Justiça da União Europeia decidiu que as regulamentações da União Europeia em matéria de proteção de dados pessoais possuem aplicação extraterritorial (KUNER, 2014; KUNER, 2017). Em essência, reafirma-se o padrão de que “a lei acompanha o dado” (KUNER, 2021).

Assim, é inevitável que surjam conflitos entre a lei que acompanha o dado nas transferências internacionais e as leis constitucionais ou de ordem pública do país de destino (KUNER, 2009a). A União Europeia, como se depreende de seus regulamentos e decisões, parece menos interessada em promover uma pauta internacional ampla de direitos à privacidade e mais focada em impor seus padrões sobre outros países (KUNER, 2009a; KUNER, 2014). A destacada postura desconsidera os possíveis impactos dessas medidas, especialmente para nações mais pobres que buscam integrar-se à globalização promovida pelas Novas Tecnologias de Informação e Comunicação (KUNER, 2014).

O direito à privacidade e o direito à proteção de dados pessoais são reconhecidos e tutelados pelo sistema internacional de direitos humanos (RENGEL, 2014; KUNER, 2014). No entanto, essa previsão, por si só, não assegura a efetividade do direito à privacidade na proteção de interesses individuais, dada a complexidade e os problemas práticos na sua implementação (KUNER, 2014).

Diante da incapacidade dos organismos internacionais em estabelecer uma regulação sólida e abrangente para o direito à privacidade nas transferências internacionais de dados pessoais, a União Europeia destacou-se como líder nesse campo (KUNER, 2014). Tal posição de protagonismo resulta, em parte, da adoção de padrões regulatórios intrusivos que, como observado por Kuner (2009a), transformam o princípio da territorialidade das jurisdições em um modelo baseado no princípio da personalidade, refletindo uma abordagem mais assertiva e abrangente.

Em outras palavras, os padrões da União Europeia acabam, de forma inevitável, obrigando outros países a observá-los (KUNER, 2014), pois, conforme o princípio de que a “lei acompanha o dado” (KUNER, 2021), esses padrões se impõem globalmente como uma ideologia jurídica unilateral e de caráter cogente (KUNER et al., 2017), sobre a qual, em regra, não houve protesto contra a afirmação jurisdicional (RYNGAERT; TAYLOR, 2020). A imposição é acompanhada pela coerção e condicionalidade de que apenas será permitido o fluxo internacional de dados com países que a União Europeia considere adequados em termos de proteção de dados pessoais (KUNER, 2017). Nesse contexto, a União Europeia demonstra não ter interesse em compreender as razões que levam outros países a adotar medidas legais divergentes (KUNER, 2017). O fenômeno destacado tem sido denominado “efeito Bruxelas” (RYNGAERT; TAYLOR, 2020; KRAMCSÁK, 2024).

Ainda que existam iniciativas de organismos internacionais para enfrentar o fenômeno discutido neste texto, como os Princípios de Privacidade da APEC, o Ato Suplementar sobre Proteção de Dados Pessoais da Comunidade Econômica dos Estados da África Ocidental e a Resolução da ONU sobre privacidade nas redes sociais, de 18 de dezembro de 2013, essas iniciativas carecem de força vinculante no âmbito jurídico internacional (KUNER, 2014; KUNER, 2010a). Nesse cenário, Kuner (2014) aponta as dificuldades em atribuir à ONU um papel significativo na promoção de esforços regulatórios internacionais sobre proteção de dados e privacidade, destacando a falta de expertise específica da organização nesse campo, dado seu caráter generalista.

Em adição, Kuner (2010a) questiona se a proteção de dados pessoais deve ser considerada um direito de natureza pública ou privada, ressaltando que essa distinção é crucial no contexto das transferências internacionais de dados. No âmbito da teoria da jurisdição, um direito à proteção de dados pessoais somente poderia ser aplicado em outra jurisdição caso fosse entendido como de natureza privada, devido às limitações impostas à aplicação extraterritorial de direitos públicos (KUNER, 2010a). Contudo, não é possível categorizar esse direito como essencialmente privado (KUNER, 2010a), especialmente pela atuação de entidades como a Autoridade Nacional de Proteção de Dados Pessoais (ANPD), que conferem um caráter público à sua regulamentação. Assim, a natureza da lei de proteção de

dados dependerá, em grande medida, do contexto de sua aplicação e do uso que se faz dela (KUNER, 2010a).

Os dilemas enfrentados pela jurisdição são inerentes a qualquer direito substantivo aplicado a questões transnacionais (SVANTESSON, 2017). Quando o debate recai sobre a internet, parece haver uma percepção equivocada de que os problemas de jurisdição são inéditos, como se uma ordem perfeita tivesse sido subitamente alterada (SVANTESSON, 2017). No entanto, esses dilemas sempre existiram no sistema internacional de direitos (SVANTESSON, 2017). Além disso, no que diz respeito à jurisdição na internet, o núcleo do problema em relação ao direito substantivo à proteção de dados pessoais ou à privacidade está intimamente ligado ao princípio da territorialidade (SVANTESSON, 2017).

Metodologicamente, não é adequado interpretar o caso *Lotus* e o *Harvard Draft* no contexto da jurisdição na internet (SVANTESSON, 2017). O método tradicional do direito exige que situações distintas sejam tratadas de maneira diferenciada (SVANTESSON, 2017). Assim, considerando que tanto o caso *Lotus* quanto o *Harvard Draft* não contemplaram o contexto da internet, sua aplicação a esse fenômeno não é metodologicamente válida (SVANTESSON, 2017). A insistência em explicar a jurisdição na internet com base nesses paradigmas não apenas falha em solucionar os desafios, mas contribui para um problema essencialmente metodológico (SVANTESSON, 2017).

Svantesson (2017) é um crítico contundente do modelo de jurisdição baseado exclusivamente no princípio da territorialidade. Ao analisar essa relação, ele destaca que a jurisdição não pode ser limitada à territorialidade, já que esta é insuficiente para resolver os conflitos complexos que frequentemente envolvem múltiplas jurisdições, colocando os Estados em posições delicadas (SVANTESSON, 2017). Além disso, as normas de direito interno que regulamentam o princípio da territorialidade carecem de clareza ao distinguir entre normas de jurisdição territorial e extraterritorial, o que agrava ainda mais a insegurança jurídica nesse contexto (SVANTESSON, 2017).

Diante da crítica ao princípio da territorialidade, Svantesson (2017) propõe, ao abordar a relação entre jurisdição e internet, três princípios fundamentais que, em sua visão, deveriam idealmente orientar as relações jurisdicionais: (I) o princípio da

conexão substancial; (II) o princípio do interesse legítimo; e (III) o princípio da razoabilidade.

No princípio da conexão substancial, destaca-se que o exercício da jurisdição deve estar fundamentado em um vínculo significativo entre o Estado que a reivindica e o conflito em questão (SVANTESSON, 2017). O princípio visa evitar alegações arbitrárias de jurisdição, exigindo que haja uma relação concreta e substancial que justifique a intervenção do Estado (SVANTESSON, 2017).

No princípio do interesse legítimo, requer-se que o Estado comprove possuir um interesse legítimo que justifique o exercício de sua jurisdição, garantindo que tal intervenção esteja alinhada com objetivos legais e éticos (SVANTESSON, 2017).

Por fim, o princípio da razoabilidade determina que o exercício da jurisdição deve buscar um equilíbrio entre a competência do Estado, os demais interesses em jogo e o interesse legítimo previamente identificado, evitando abusos e garantindo proporcionalidade (SVANTESSON, 2017).

A territorialidade jurisdicional não é uma condição indispensável para a existência do Estado, ou seja, o Estado pode continuar a existir territorialmente mesmo que sua jurisdição se baseie em outros princípios (SVANTESSON, 2017). É preciso ressaltar, no entanto, que não se aborda a extinção do princípio da territorialidade, mas um declínio ontológico de sua estrutura rígida, que historicamente tem sido interpretada como o único fundamento explicativo para o fenômeno e a aplicação da jurisdição (SVANTESSON, 2017). Nesse sentido, o princípio da territorialidade da jurisdição continuará a existir, mas deixará de ser a principal justificativa ou causa para o exercício jurisdicional extraterritorial (SVANTESSON, 2017). Em seu lugar, o exercício da jurisdição será fundamentado nos princípios supracitados, como a conexão substancial, o interesse legítimo e a razoabilidade (SVANTESSON, 2017).

Svantesson (2017) destaca a necessidade de estabelecer uma interoperabilidade jurisdicional que, simultaneamente, abarque uma interoperabilidade jurídica. Tal abordagem busca consolidar as semelhanças entre os sistemas jurídicos existentes e superar suas diferenças (SVANTESSON, 2017). Nesse sentido, ao invés de aspirar ao utópico ideal de um tratado ou convenção internacional que uniformize os temas discutidos neste texto, deve-se valorizar a construção de um “sistema” formado por “sistemas jurídicos distintos”

(SVANTESSON, 2017). Sistemas que, embora diferentes entre si, podem operar de maneira efetiva e com poucos conflitos, representando um avanço significativo para a regulação das transferências internacionais de dados pessoais (SVANTESSON, 2017).

Na era da hiper-regulamentação, previamente abordada, um aspecto relevante foi o surgimento do conceito de jurisdição corretiva, que estabelece os parâmetros que justificam onde e em quais circunstâncias uma ordem judicial pode ser executada (SVANTESSON, 2017). O debate decorre de dois tipos principais de jurisdição: a jurisdição *in persona*, que diz respeito à legitimidade de um tribunal para julgar uma parte específica, e a jurisdição por assunto, que trata da competência temática de um tribunal para decidir sobre determinado caso (SVANTESSON, 2017).

Entender a questão colocada é crucial para a transferência internacional de dados pessoais, pois, embora a ANPD detenha jurisdição por assunto e possa julgar as partes envolvidas, é o escopo da jurisdição corretiva que determinará o alcance e a natureza das medidas que podem ser adotadas. Contudo, esse escopo apresenta barreiras significativas, especialmente diante da remoção global de conteúdos na internet, que demonstra como a autocontenção do escopo da jurisdição corretiva tem sido comprometida pelo avanço de decisões judiciais com efeitos extraterritoriais em casos relacionados à internet (SVANTESSON, 2017).

Os legisladores devem adotar uma postura razoável em suas reivindicações de jurisdição, regulando apenas o necessário e evitando extrapolações desproporcionais que invadam a jurisdição de outros países (SVANTESSON, 2017). No contexto das transferências internacionais de dados, Svantesson (2017; 2013) propõe que as reivindicações de jurisdição observem três camadas fundamentais: I) a camada de prevenção de abusos (*the abuse-prevention layer*); II) a camada de direitos (*the rights layer*); e III) a camada administrativa (*the administrative layer*).

Na camada de prevenção de abusos, Svantesson (2017; 2013) explica que um Estado pode exercer jurisdição sobre condutas na internet desde que tenha controle sobre o mercado relacionado à conduta, o que autoriza a aplicação de jurisdição extraterritorial. Na camada de direitos, deve-se avaliar o grau de contato entre o agente envolvido e o Estado que busca expandir sua jurisdição (SVANTESSON, 2017; SVANTESSON, 2013). Já a camada administrativa analisa a existência de um vínculo suficientemente significativo entre o direito à privacidade e

o Estado que reivindica a jurisdição, sendo essencial para determinar se esse vínculo justifica o exercício jurisdicional (SVANTESSON, 2017; SVANTESSON, 2013).

As transferências internacionais de dados pessoais representam um desafio jurídico que exige a superação de modelos tradicionais de jurisdição, como o princípio da territorialidade, em favor de abordagens mais flexíveis e adaptadas à era digital. A personalização da jurisdição e os esforços por interoperabilidade entre sistemas jurídicos surgem como respostas às complexidades do fluxo global de dados, embora gerem conflitos extraterritoriais e incertezas regulatórias. Iniciativas como as da União Europeia evidenciam o protagonismo de regimes normativos unilaterais, mas também expõem a necessidade de uma governança global mais equilibrada, que harmonize a proteção do direito à privacidade com a dinâmica do comércio digital e respeite as peculiaridades dos diferentes sistemas legais.

3.2 O DIREITO À PRIVACIDADE COMO NORMA *JUS COGENS* NO SISTEMA INTERNACIONAL DE DIREITOS HUMANOS E IMPACTOS PARA A TRANSFERÊNCIA INTERNACIONAL DE DADOS

A privacidade, enquanto direito, é amplamente reconhecida no âmbito dos direitos humanos, não apenas como uma proteção individual, mas também como um pilar essencial para a dignidade humana e para o exercício de outras liberdades fundamentais. Conforme visto no subitem 2.1 deste documento, a privacidade é intrínseca à estrutura da liberdade individual, sendo indispensável para a preservação da autonomia. Assim, a relevância internacional do Direito à Privacidade, enquanto um Direito Humano, é de extrema importância para este trabalho, uma vez que os Direitos Humanos representam o núcleo duro dos Direitos Fundamentais consagrados nas Constituições de tradição liberal (DIGGELMANN; CLEIS, 2014). Proteger a privacidade significa permitir que as pessoas se resguardem de intervenções externas, sejam elas provenientes do Estado ou de outros indivíduos, reforçando os argumentos de Diggelmann e Cleis (2014), Rengel (2014), Roessler (2017) e Bagahi (2012) de que esse direito é imprescindível para uma vida digna e para o pleno desenvolvimento pessoal.

Nesse mesmo sentido, a digitalização evidenciou ainda mais a necessidade de proteger a privacidade não apenas como um conceito abstrato, mas com a

implementação de mecanismos concretos que assegurem sua preservação diante das inovações tecnológicas (vide discussões do item 2 deste documento) (SLOOT, 2017b).

Svantesson (2017) destaca que as regras de jurisdição devem respeitar os direitos humanos, o que implica que as transferências internacionais de dados pessoais não podem ocorrer de forma a violar o direito à privacidade. Nesse contexto, Ramiro (2022) afirma que o direito à proteção de dados pessoais, seja explícita ou implicitamente, está reconhecido como um direito humano, por ser uma extensão direta do direito à privacidade, amplamente consolidado no Direito Internacional dos Direitos Humanos. O processo de internacionalização do direito à privacidade reforça a ideia de que a privacidade não é um direito secundário, mas um elemento essencial para a manutenção da convivência democrática (KRAMER, 2024).

Ainda que cada país lide com a privacidade de forma peculiar (BOSHE, 2015), o reconhecimento internacional do direito à privacidade é amplamente refletido em diversas convenções e tratados de direitos humanos, como a Declaração Universal dos Direitos Humanos de 1948 e o Pacto Internacional sobre Direitos Civis e Políticos de 1966, ambos consagrando a privacidade como um direito essencial e fundamental (KUNER, 2010c; KUNER et al., 2011; CARRASQUILLA, 2012; DIGGELMANN; CLEIS, 2014; KURAT, 2023a; KURAT, 2023b; KRAMER, 2024). Rengel (2013) complementa essa visão ao destacar a relevância de outros instrumentos internacionais, como a Convenção sobre os Direitos da Criança, a Declaração Americana dos Direitos e Deveres do Homem, a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, a Carta dos Direitos Fundamentais da União Europeia e a Carta Africana dos Direitos Humanos e dos Povos, que reforçam o compromisso global com a proteção da privacidade como um elemento central na garantia da dignidade e das liberdades individuais.

Nesse contexto, a privacidade, atualmente, assume uma posição central que, em outras épocas, foi ocupada pelos direitos trabalhistas e pelos direitos do consumidor (KUNER et al., 2013a; KUNER et al., 2019). A concepção da privacidade como um direito humano traz implicações jurídicas profundas, pois, ao fortalecer sua proteção, dificulta-se sua flexibilização para atender interesses econômicos, refletindo uma priorização crescente dos direitos individuais (KUNER, 2010c).

Com o advento das tecnologias de informação e comunicação, a privacidade adquire uma dupla dimensão, pois se torna uma arena de disputas entre os interesses dos direitos humanos e as pressões do mercado (KUNER, et al., 2011; CATE et al., 2012; KRAMER, 2024). A intensificação dessas tecnologias coloca o direito à privacidade no centro de um novo debate sobre a proteção da esfera individual frente às demandas econômicas, ao mesmo tempo em que desafia os modelos de regulação existente (KUNER, et al., 2011; CATE et al., 2012).

No campo da transferência internacional de dados pessoais, a OCDE desempenhou um papel pioneiro ao publicar suas Diretrizes de Privacidade em 1980, fornecendo um marco para equilibrar a proteção da privacidade com o livre comércio (SUDA, 2017; ANGARITA; ZULUAGA, 2019; KUNER, 2010c). Nessas diretrizes, a OCDE recomendou que os países-membros implementassem princípios fundamentais de proteção de dados, como a limitação da coleta e a definição clara das finalidades do tratamento (SUDA, 2017; CATE; MAYER-SCHÖNBERGER, 2013). Além disso, destacou que a circulação de dados entre países com níveis de proteção equivalentes deve ser livre, permitindo restrições apenas para resguardar a privacidade dos indivíduos (KUNER, 2010c).

A abordagem ganha ainda mais relevância diante da possibilidade de as transferências internacionais de dados serem interpretadas como barreiras ao comércio no âmbito do Acordo Geral sobre Comércio de Serviços (GATS) (KUNER, 2010c; CELLI, 2020). Embora o GATS não regule diretamente essas transferências, os conflitos decorrentes podem ser levados à Organização Mundial do Comércio (OMC), evidenciando a interseção entre proteção de dados e comércio internacional (KUNER, 2010c). A título de exemplo, Oldani (2020) descreve a noção de protecionismo de dados, em que a proteção de dados é empregada como um mecanismo para resguardar os mercados nacionais de tecnologias e inovação.

Em 2004, a Cooperação Econômica Ásia-Pacífico (APEC) avançou significativamente ao criar o Quadro de Privacidade, abrangendo 21 economias e estabelecendo diretrizes para a proteção da privacidade (KUNER, 2010a; KUNER, 2009b), refletindo a crescente relevância do direito à privacidade no contexto do comércio internacional, ao buscar harmonizar padrões de proteção de dados com as necessidades econômicas e comerciais da região (KUNER, 2010a; KUNER, 2009b).

À luz disso, a regulação da transferência internacional de dados pessoais transcende a esfera puramente jurídica, conectando-se profundamente aos processos econômicos globais (KUNER, 2010a; KUNER, 2009b). Em 1990, as Nações Unidas (ONU) elaboraram diretrizes sobre arquivos pessoais computadorizados que, embora não tenham caráter vinculativo, representam um marco relevante para a compreensão da circulação transfronteiriça de dados (KUNER, 2010c; ANGARITA; ZULUAGA, 2019). Segundo as diretrizes da ONU, a transferência de dados deve ocorrer entre países que assegurem níveis de proteção adequados, consolidando o princípio de salvaguarda do direito à privacidade como pilar fundamental (KUNER, 2010c).

Em síntese, o direito à privacidade, como direito humano, não apenas assegura a proteção da esfera pessoal e a autonomia dos indivíduos, mas também apresenta desafios relevantes para a regulação das transferências internacionais de dados. Está profundamente interligado à tensão entre a proteção dos dados pessoais e as exigências globais de comércio e inovação tecnológica. O fortalecimento dessa proteção, por meio de tratados internacionais e iniciativas como as da OCDE e da APEC, destaca a crescente relevância do direito à privacidade no cenário global.

No que diz respeito ao direito à privacidade no direito internacional, Rengel (2013) argumenta que esse direito não pode ser classificado como uma norma de *jus cogens*, uma vez que sua violação, segundo a autora, não configura uma infração grave aos direitos humanos. Contudo, considerando a relevância crescente da privacidade na atualidade, a perspectiva arguida demanda uma reavaliação.

O direito à privacidade, reconhecido como um direito fundamental, possui uma importância que ultrapassa fronteiras nacionais e culturais e, conforme descrito anteriormente, é assegurado por diversos instrumentos normativos internacionais. A noção de *jus cogens*, conforme explicado por Linderfalk (2013), diz respeito a normas de direito internacional de caráter imperativo, que não podem ser modificadas ou revogadas por tratados ou acordos entre Estados. Assim, tratar o direito à privacidade como uma norma *jus cogens* implica atribuir-lhe uma proteção absoluta e intransigente, que deve ser respeitada em âmbito global.

O conceito de *jus cogens* enfatiza a hierarquia superior dessas normas no sistema jurídico internacional (KRAMER, 2024; KURAT, 2023a; KURAT, 2023b;

LINDERFALK, 2013). Ao aplicar essa perspectiva ao direito à privacidade, conclui-se que este não pode ser negociado. De acordo com esse atributo, consolida-se a visão de que a privacidade deve ser considerada um direito inalienável, protegendo a autonomia individual contra eventuais abusos, seja por parte do Estado ou de agentes privados.

Kramer (2024) ressalta que, no contexto digital, a privacidade ganha uma relevância ainda mais central, porque o acesso ilimitado a dados pessoais e o avanço da vigilância tornam imprescindível a proteção da privacidade para assegurar a liberdade e a dignidade humanas. Assim, enxergar o direito à privacidade como uma norma *jus cogens* não apenas reforça sua importância como direito individual, mas também o eleva à condição de pilar fundamental de uma sociedade democrática, comprometida com a liberdade e os direitos fundamentais de todos os cidadãos (KRAMER, 2024).

Hodiernamente, com o avanço das tecnologias de informação e comunicação, o direito à privacidade assume um papel ainda mais crucial, especialmente em situações de vulnerabilidade, como no caso do uso de Tecnologias de Informação e Comunicação em zonas de conflito. Conforme apontam Kuner et al. (2017), Magalhães e Couldry (2021) e Lucas Gonçalves da Silva e Reginaldo Felix Nascimento (2023), essas tecnologias têm sido amplamente utilizadas para apoiar iniciativas humanitárias em zonas de conflito e refúgio. No entanto, esse avanço também eleva significativamente o risco de vazamento de dados pessoais desses indivíduos. A exposição dos registros de sujeitos em tais áreas pode se transformar em uma ferramenta perigosa para perseguições políticas, colocando em risco não apenas a segurança e vida dos próprios refugiados, mas também de seus familiares (MAGALHÃES; COULDRY, 2021; SILVA; NASCIMENTO, 2023). Nesse contexto, a privacidade transcende a dimensão de uma escolha individual, tornando-se uma salvaguarda essencial para a proteção de vidas.

Portanto, ao reconhecer o direito à privacidade como uma norma *jus cogens*, afirma-se sua função essencial na proteção da dignidade humana e na garantia da liberdade individual, especialmente em contextos de extrema vulnerabilidade, como o vivido nas zonas de conflito. O direito à privacidade, por sua natureza e relevância, não é passível de negociação ou relativização, exigindo proteção com a mesma força e prioridade atribuídas às demais normas fundamentais do direito internacional.

A concepção do direito à privacidade como uma norma de *jus cogens* impacta profundamente a Transferência Internacional de Dados, ao estabelecer uma proteção universal que transcende barreiras jurídicas e culturais (KRAMER, 2024). No contexto da Transferência Internacional de Dados, pode-se concluir que tais operações devem necessariamente respeitar padrões globais de proteção à privacidade, vedando a movimentação de dados para países cujas legislações não garantam esse direito de forma adequada. Nesse mesmo sentido, a partir da perspectiva de Kramer (2024), essa interpretação é essencial para garantir que a privacidade dos indivíduos seja respeitada, independentemente das jurisdições envolvidas nas transferências.

A hierarquia jurídica das normas *jus cogens* coloca a proteção da privacidade em um patamar superior a outras demandas, incluindo os interesses econômicos e do mercado, impedindo que violações sejam justificadas sob o pretexto de conveniência (KURAT, 2023a; KURAT, 2023b; KRAMER, 2024). No âmbito das Transferências Internacionais de Dados, isso implica que qualquer movimentação de dados pessoais deve estar estritamente alinhada às normas internacionais de privacidade. No cenário digital atual, onde o acesso irrestrito a informações pessoais se tornou uma prática comum, o direito à privacidade precisa ser tratado como uma prioridade absoluta (KRAMER, 2024).

Kuner et al. (2017) destacam que, com o avanço acelerado da digitalização e a intensificação da coleta de dados pessoais, a privacidade se tornou um direito vulnerável, demandando uma regulação sólida para assegurar que os fluxos de dados não comprometam a dignidade dos indivíduos. A ideia da privacidade como norma de *jus cogens* sublinha a necessidade de um regime jurídico global capaz de proteger os dados pessoais em todas as jurisdições, evitando transferências internacionais de dados sem as garantias adequadas de segurança.

Por fim, a concepção do direito à privacidade como norma de *jus cogens* determina que sua proteção seja universal e intransigente, refletindo diretamente nas práticas de Transferência Internacional de Dados. A partir da perspectiva de Linderfalk (2013), Kramer (2024) e Kurat (2023a; 2023b), é possível sustentar que, enquanto norma imperativa, a privacidade não pode ser subordinada a outras prioridades jurídicas, como normas que busquem priviliegiar interesses econômicos. No contexto digital, o direito à privacidade se consolida como um pilar essencial dos

direitos humanos, exigindo uma regulação robusta e eficaz que assegure sua proteção (KRAMER, 2024), independentemente das fronteiras ou pressões econômicas.

3.3 A TRANSFERÊNCIA INTERNACIONAL DE DADOS: UNIÃO EUROPEIA E AMÉRICA LATINA

Na Europa, a União Europeia e o Conselho da Europa desempenharam papéis essenciais na consolidação do Direito à Proteção de Dados Pessoais (TERWANGNE, 2022). A proteção de dados foi inicialmente prevista no art. 8º do Convênio Europeu de Direitos Humanos de 1950. Esse marco inicial foi seguido por importantes avanços legislativos, como a Convenção 108 de Tratamento de Dados Pessoais, adotada em 1981, a Diretiva 95/46 da Comissão Europeia e, mais recentemente, o Regulamento Geral de Proteção de Dados (RGPD). O RGPD não é apenas um regulamento com objetivos internos, mas também possui mecanismos que, inevitavelmente, expandem sua influência globalmente (BÚRCA, 2019).

A Convenção 108, promovida pelo Conselho da Europa, destaca-se como uma das primeiras medidas abrangentes na proteção de dados pessoais, especialmente por permitir sua assinatura por países não europeus, ampliando seu alcance global (TERWANGNE, 2022; KUNER, 2010c; ANGARITA; ZULUAGA, 2019). Posteriormente, a mencionada Convenção foi revisada com disposições específicas sobre Transferência Internacional de Dados, reforçando seu papel como instrumento jurídico fundamental para a proteção da privacidade em um contexto globalizado (TERWANGNE, 2022; KUNER, 2010c; ANGARITA; ZULUAGA, 2019; HERT; GUTWIRTH, 2009).

A Diretiva 95/46/CE foi uma das iniciativas mais significativas para a harmonização do direito europeu no campo da proteção de dados pessoais (TERWANGNE, 2022; KUNER, 2010c). Sua importância foi tamanha que, em 2016, passou por uma transformação substancial, sendo convertida em um regulamento com as adaptações necessárias, culminando no surgimento do GDPR (*General Data Protection Regulation*)(TERWANGNE, 2022; KUNER, 2010c).

Nesse cenário, a transferência internacional de dados pessoais é regulada tanto pelo GDPR quanto pela Convenção 108+ (TERWANGNE, 2022). Embora o GDPR não forneça uma definição explícita do termo “fluxo transfronteiriço de dados”,

o *Explanatory Memorandum* da Convenção 108+ esclarece que essas transferências ocorrem sempre que dados pessoais são acessados ou compartilhados com um destinatário localizado em jurisdição estrangeira, seja em outro Estado ou em uma Organização Internacional (TERWANGNE, 2022).

A Convenção 108+ apresenta um caráter ambicioso ao estender a aplicação de suas disposições não apenas aos Estados signatários, mas também àqueles que não integram formalmente o acordo (TERWANGNE, 2022). Apesar de promover maior interoperabilidade entre os signatários, a Convenção condiciona o fluxo de dados à adoção de medidas e padrões europeus, sem levar em consideração as especificidades normativas de diferentes sistemas jurídicos (TERWANGNE, 2022). Nesse contexto, pode-se interpretar que a Europa busca, em certa medida, resguardar-se frente às demais jurisdições, reforçando sua autonomia regulatória (KUNER, 2020e).

Dessa forma, nas transferências de dados destinadas a países fora da jurisdição da Convenção, é exigido que o destinatário estrangeiro garanta um nível adequado de proteção aos dados, alinhado aos padrões estabelecidos pelas normativas europeias (TERWANGNE, 2022; KUNER, 2010c). Por conseguinte, o GDPR expande as bases legais que possibilitam a transferência internacional de dados para fora da União Europeia (BERTONI, 2020), fundamentando-se, entre outros critérios, na decisão de adequação emitida pela Comissão Europeia ou na garantia oferecida pelo exportador por meio de salvaguardas apropriadas, como regras corporativas vinculantes, cláusulas-padrão contratuais e outros mecanismos equivalentes (TERWANGNE, 2022; KUNER, 2012).

Na ausência de salvaguardas apropriadas ou de uma decisão de adequação, o GDPR ainda permite a transferência internacional de dados em situações excepcionais, como quando ocorre o consentimento explícito do titular, a execução de contratos no interesse do titular, interesses públicos relevantes, a defesa de reivindicações legais ou para a proteção de interesses vitais (TERWANGNE, 2022; KUNER, 2012; KUNER, 2020f).

Adicionalmente, no âmbito do Direito Europeu, o GDPR determina, em seu art. 27, a obrigatoriedade de que tanto o processador quanto o controlador, situados fora da União Europeia, designem representantes em território europeu para assegurar a conformidade com as normas de proteção de dados (KUNER, 2021).

Na Europa, assim como ocorreu com o Direito à Privacidade discutido no capítulo anterior, o avanço nas regras sobre Transferência Internacional de Dados também se evidencia pela evolução jurisprudencial do Tribunal de Justiça da União Europeia (TJUE) (KUNER, 2021). No caso *Lindqvist*, o tribunal determinou que não se configurava Transferência de Dados para um país terceiro, nos termos da Diretiva de Proteção de Dados, quando um agente de um Estado-membro carregava dados pessoais em uma página da internet hospedada dentro da União Europeia (KUNER, 2021; KUNER, 2020a). Em outras palavras, o tribunal definiu que é necessário haver um envio ativo para que se caracterize a Transferência Internacional de Dados, e que a simples disponibilização passiva de dados na internet não atende a esse critério (KUNER, 2020a). O julgamento *Lindqvist* marcou o início da delimitação dos critérios para a Transferência Internacional de Dados Pessoais (KUNER, 2021).

Conforme mencionado no item 3.1 deste documento, a jurisdição de privacidade da União Europeia fundamenta-se no princípio da personalidade, segundo o qual o direito acompanha o dado (KUNER, 2009a). Diante dessa abordagem, os Estados Unidos consideraram que os padrões impostos pela União Europeia eram excessivamente invasivos e incompatíveis com a concepção de privacidade adotada pelo ordenamento jurídico estadunidense (SUDA, 2017). Para mitigar essa discordância, foi estabelecido o *Safe Harbor*, um acordo bilateral entre os Estados Unidos e a União Europeia, com o objetivo de harmonizar as diferenças transnacionais e equilibrar a extensão da jurisdição europeia sobre a proteção de dados (SUDA, 2017; KUNER, 2010c).

No julgamento do caso *Schrems I*, o Tribunal de Justiça da União Europeia invalidou a decisão que autorizava a transferência internacional de dados entre a União Europeia e os Estados Unidos com base no *Safe Harbor* (KUNER, 2021; KUNER et al., 2016). A decisão determinou que as transferências internacionais devem observar padrões mais rigorosos de proteção, reafirmando a essencialidade da proteção de dados pessoais como um direito fundamental (KUNER, 2021; KUNER et al., 2016). O tribunal enfatizou que o nível de proteção nos países destinatários deve ser juridica e ontologicamente equivalente aos padrões europeus (KUNER, 2021).

No *Schrems I*, ficou evidente que o critério de análise das violações de dados pessoais em transferências internacionais não é subjetivo (KUNER, 2020a). Tal

circunstância revela que a avaliação não considera a intenção do agente em causar a violação, mas se baseia em elementos objetivos. Em outras palavras, qualquer transferência internacional de dados deve, obrigatoriamente, cumprir os padrões europeus de proteção de dados, independentemente das intenções do agente envolvido (KUNER, 2020a).

Na avaliação do *Schrems II*, o Tribunal de Justiça da União Europeia declarou inválida a decisão da Comissão Europeia que reconhecia a adequação do *Privacy Shield* entre a União Europeia e os Estados Unidos (KUNER, 2021; KUNER et al., 2016; MANTOVANI, 2020). O Tribunal ressaltou que o artigo 46 do GDPR impõe a exigência de que o nível de proteção garantido em transferências internacionais seja equivalente ao padrão europeu. Para tanto, destacou-se a necessidade de adoção de medidas práticas e efetivas que assegurem essa equivalência de proteção (KUNER, 2021). A partir dos *Schrems* I e II, percebe-se como a questão da transferência internacional de dados é, de mandeira prevalescente, jurisdicional, onde o exercício jurisdição como forma de soberania acaba oferecendo barreiras para o sucesso da transferência (COCHE; KOLK; OCELÍK, 2024).

No Parecer 1/15, a Corte concluiu que o acordo internacional proposto para a transferência internacional de dados de passageiros aéreos ao Canadá não poderia ser aprovado por estar em desacordo com os padrões de proteção de dados da União Europeia (KUNER, 2021). Além disso, foi estabelecido que, mesmo quando a transferência internacional de dados for subsequente, ela deve estar em conformidade com os padrões europeus de proteção de dados, assegurando a manutenção de um nível equivalente de proteção (KUNER, 2020a).

No julgado *Google Spain*, o Tribunal de Justiça da União Europeia determinou que o processamento de dados realizado por uma empresa sediada fora da União Europeia, mas com filial em território europeu, está sujeito à legislação de proteção de dados da União Europeia, mesmo que as atividades dessa filial estejam economicamente vinculadas a um operador global, como no caso do Google (KUNER, 2021). Posteriormente, no caso *Google LLC*, o Tribunal reafirmou essa posição, estabelecendo que operações de mecanismos de busca em países terceiros, quando intrinsecamente conectadas a filiais localizadas dentro da União Europeia, também estão sujeitas à aplicação do GDPR, reforçando o alcance extraterritorial da legislação europeia de proteção de dados (KUNER, 2021).

O GDPR aborda a transferência internacional de dados em seu Capítulo V (KUNER, 2020a). O art. 44, que substitui o art. 25 da antiga Diretiva de Proteção de Dados da União Europeia, estabelece o princípio fundamental da transferência internacional de dados, definindo que ela deve ocorrer em duas etapas (KUNER, 2020a). Isso denota que, antes de efetivar a transferência (segunda etapa), o destinatário dos dados precisa demonstrar conformidade com todas as exigências do GDPR (primeira etapa), indo além das normas específicas sobre transferências internacionais de dados (KUNER, 2020a). Em outras palavras, o GDPR busca evitar que a transferência internacional de dados seja usada como mecanismo para contornar suas regras de proteção (KUNER, 2020a). O princípio reflete uma vedação à evasão da lei, garantindo que os padrões europeus de proteção de dados sejam preservados independentemente da localização do processamento (KUNER, 2020a; KUNER, 2009b).

O art. 45 do GDPR regula a Transferência Internacional de Dados com base em uma decisão de adequação (KUNER, 2020b; SULLIVAN, 2019). Consoante descreve Kuner (2019), para que uma regulação de dados precise ser considerada adequada, ela não precisa ser idêntica, porém, necessita ser semelhante ao padrão europeu. Assim, a União Europeia impõe seu padrão, mas sem pretender ofender diretamente a soberania regulatória dos países terceiros. Nesse contexto, a decisão de adequação fundamenta-se na avaliação de similaridade entre o ordenamento jurídico do país destinatário ou organização e os padrões de proteção de dados estabelecidos pela União Europeia (KUNER, 2020b; SULLIVAN, 2019; JULIUSSEN et al., 2023). Além disso, o art. 45 reflete como o Direito à Proteção de Dados Pessoais foi moldado pela jurisprudência do Tribunal de Justiça da União Europeia, considerando que as condições para a emissão de uma decisão de adequação foram amplamente influenciadas pelos princípios estabelecidos no caso *Schrems* (KUNER, 2020b). No entanto, deve-se acrescentar que os critérios ainda são vagos e necessitam de maior transparência (WAGNER, 2018).

Ademais, no caso *Schrems I*, o Tribunal de Justiça da União Europeia determinou que a decisão de adequação deve ser submetida a uma revisão periódica, o que está devidamente ratificado pelo art. 45 do GDPR (KUNER, 2020b). Isso reforça a necessidade de monitoramento constante para garantir que o nível de

proteção no país ou organização destinatária permaneça compatível com os padrões europeus de proteção de dados (KUNER, 2020b).

Quando uma transferência internacional de dados não puder ser realizada com base no art. 45 do GDPR, ela poderá ser viabilizada através das salvaguardas previstas no art. 46 (KUNER, 2020b; KUNER, 2020c). As salvaguardas incluem cláusulas contratuais padrão, cláusulas *ad hoc* ou normas corporativas globais vinculativas, garantindo que o nível de proteção exigido pela União Europeia seja mantido mesmo em jurisdições externas (KUNER, 2020c).

Nas cláusulas-padrão contratuais, a Comissão Europeia disponibiliza, por meio de decisão, um modelo contratual para regulamentar a transferência internacional de dados, o qual deve ser integralmente respeitado e não pode ser alterado (KUNER, 2020c). Caso sejam feitas alterações nesse modelo, as cláusulas deixam de ser consideradas padrão e passam a ser classificadas como cláusulas *ad hoc* (KUNER, 2020c).

As cláusulas *ad hoc*, diferentemente das cláusulas-padrão contratuais, são elaboradas para atender a contextos específicos e necessitam de aprovação prévia por parte da autoridade de proteção de dados pessoais competente (KUNER, 2020c).

O art. 46 do GDPR também prevê a possibilidade de transferência internacional de dados com base em instrumentos juridicamente vinculativos e executáveis (KUNER, 2020c). Nesse sentido, o GDPR permite a celebração de acordos internacionais específicos para regular a Transferência Internacional de Dados e assegur a Proteção de Dados Pessoais (KUNER, 2020c).

Ademais, o art. 46 do GDPR menciona a possibilidade de utilizar Códigos de Conduta para Transferência Internacional de Dados, os quais necessitam de aprovação pela Comissão Europeia (KUNER, 2020c). Além disso, no caso dos mecanismos de certificação, estes devem ser aprovados por uma autoridade de proteção de dados pessoais ou por uma entidade de certificação competente, garantindo conformidade com os padrões europeus de proteção de dados (KUNER, 2020c).

A inclusão de disposições em acordos administrativos para a transferência internacional de dados está disposta no art. 46 do GDPR, ainda que esses acordos não possuam natureza vinculativa (KUNER, 2020c). Contudo, isso gera uma

aparente contradição, já que é desafiador conceber como os direitos relacionados à proteção de dados poderiam ser executados de forma efetiva com base em acordos que carecem de força vinculativa (KUNER, 2020c).

Dessarte, o artigo 47 do GDPR trata das regras corporativas globais, que nada mais são do que políticas internas de proteção de dados adotadas por empresas ou grupos empresariais para regular a transferência de dados pessoais para países fora da União Europeia (KUNER, 2020d). As regras são aplicáveis tanto a controladores quanto a processadores localizados em um Estado-Membro da UE, sempre que lidam com dados pessoais em transferências internacionais dentro do mesmo grupo empresarial ou em parcerias econômicas conjuntas (KUNER, 2020d). O objetivo dessas regras é garantir que os dados pessoais estejam protegidos mesmo fora da União Europeia (KUNER, 2020d). Para isso, o artigo detalha as condições que devem ser cumpridas, promovendo um padrão uniforme de proteção que transcende fronteiras e assegura a privacidade em âmbito global (KUNER, 2020d).

Mantovani (2020) descreve que, ainda que tais contratos passem pelo crivo de uma autoridade pública, eles não perdem seu caráter essencialmente privado. Surge, assim, o contrato como instrumento de governança, fundamentando o movimento de contratualização da sociedade na contemporaneidade (MANTOVANI, 2020). Com efeito, observa-se a desvirtuação dos contratos em relação à sua natureza tradicional, uma vez que, agora, são instrumentalizados para a organização política da sociedade (MANTOVANI, 2020) e como um modo de exercício da soberania.

Mantovani (2020) elucida que o contratualismo de transferência internacional de dados não permite apenas a transferência do dado europeu, mas também a exportação do Direito Europeu pelo contrato. Isso ocorre porque a utilização do contrato para a transferência internacional de dados estabelece um território contratual (MANTOVANI, 2020). À vista disso, o território contratual é resultado dos termos acordados entre as partes, molda a conduta daqueles que interagem nesse espaço geográfico e influencia os eventos que ocorrem em seu interior, os quais, posteriormente, serão juridicamente avaliados (MANTOVANI, 2020). Logo, percebe-se como a jurisdição europeia se estende por meio da contratualização das relações na sociedade internacional (MANTOVANI, 2020).

A partir da perspectiva de Mantovani (2020), a descentralização observada da soberania estatal, por meio da privatização da normatividade, deve ser percebida como uma forma de refeudalização das relações sociais, em consonância com a tese defendida por Olaf Kaltmeier (2020), pois evidencia uma governança fragmentada e fundamentada em relações contratuais.

O artigo 48 do GDPR trata das transferências ou divulgações de dados pessoais que não são autorizadas pela legislação da União Europeia (KUNER, 2020e). O supracitado artigo é frequentemente referido como um “estatuto de bloqueio” devido à sua função de proteger o espaço jurídico europeu contra a interferência de jurisdições de países terceiros (KUNER, 2020e). Ele estabelece barreiras para impedir que ordens ou decisões judiciais emitidas por autoridades estrangeiras possam forçar a transferência de dados pessoais para fora da União Europeia, a menos que estejam em conformidade com os padrões de proteção de dados da UE (KUNER, 2020e). Assim, o artigo 48 assegura que a legislação europeia continue sendo respeitada e impede que outros regimes jurídicos menos rigorosos comprometam os padrões de privacidade e proteção de dados estabelecidos pelo GDPR (KUNER, 2020e).

Assim, o artigo 48 do GDPR representa um marco significativo na proteção de dados pessoais e no contexto das transferências internacionais de dados, destacando-se como o primeiro estatuto de bloqueio integrado a uma legislação de proteção de dados pessoais (KUNER, 2020e). Nesse sentido, o estatuto de bloqueio é acionado sempre que uma decisão judicial ou administrativa de um país terceiro, com efeito extraterritorial, exigir que um controlador ou processador de dados sob a jurisdição da União Europeia transfira ou divulgue dados pessoais regidos pelo GDPR (KUNER, 2020e). A destacada disposição reforça a soberania regulatória da União Europeia, ao garantir que qualquer transferência de dados respeite os padrões de proteção europeus, mesmo diante de pressões externas (KUNER, 2020e).

No artigo 49 do GDPR, constatam-se hipóteses de derrogações aplicáveis a situações específicas (KUNER, 2020f). As transferências realizadas com base nessas derrogações devem ocorrer em *ultima ratio*, ou seja, apenas quando nenhuma das hipóteses anteriores for aplicável (KUNER, 2020f; MARELLI, 2023).

Nesse diapasão, o art. 49 do GDPR reflete um declínio ontológico ao evidenciar a honestidade normativa da lei em reconhecer que o Direito à Proteção de

Dados Pessoais não é absoluto e pode ser relativizado diante de direitos de interesse social mais preponderante (KUNER, 2020f). Por exemplo, o artigo permite a transferência internacional de dados para proteger o interesse vital do titular dos dados pessoais (KUNER, 2020f). Nesse caso, a proteção de dados é relativizada em prol de um direito superior, como o direito à vida (KUNER, 2020f). Na pandemia, a transferência internacional de dados desempenhou um papel crucial no enfrentamento da Covid-19 (BENTZEN; OLAV; URSIN, 2023; KIDWELL, 2023).

Observa-se, assim, discussões sobre ser legítimo o interesse da coleta massiva de informações com justificativa na crise climática, que exige a transferência internacional de dados para ações coordenadas (KIDWELL, 2023). Um exemplo é o *Executive Order* 14086 (EUA) – *Enhancing Safeguards For United States Signals Intelligence Activities*–, que aborda a coleta de informações para a compreensão das ameaças oferecidas pelas mudanças climáticas (KIDWELL, 2023).

A cooperação internacional voltada à proteção de dados pessoais está disposta no art. 50 do GDPR (KUNER, 2020g). Nesse contexto, é importante destacar que o artigo não impõe restrições para que os Estados-Membros celebrem acordos internacionais com países terceiros, visando regular as transferências internacionais de dados pessoais e fortalecer a proteção desses dados em escala global (KUNER, 2020g).

Assim, o supracitado dispositivo reforça a cooperação internacional na proteção de dados pessoais, permitindo que os Estados-Membros celebrem acordos internacionais com países terceiros, desde que tais acordos não violem as disposições do GDPR, consolidando o princípio de vedação à evasão da lei nas transferências internacionais de dados pessoais (KUNER, 2020g). Nesse contexto, além de priorizar o aspecto da reciprocidade, o GDPR adota o princípio da conformidade como diretriz essencial para orientar a cooperação internacional da União Europeia em matéria de proteção de dados pessoais (KUNER, 2020g).

Laconicamente, o padrão europeu, frequentemente denominado como o “padrão ouro” devido ao seu status de referência mundial em matéria de proteção de dados pessoais, enfrenta desafios significativos na aplicação transnacional do GDPR, mesmo dentro do próprio território europeu (GENTILE; LYNSKEY, 2022). Apesar de sua pretensa sofisticação, o GDPR apresenta falhas atribuídas a um *design* problemático, que podem ser sintetizadas em quatro principais deficiências: I)

ambiguidades e divergências no processo de cooperação entre as Autoridades Nacionais de Supervisão (NSAs); II) ausência de igualdade entre essas autoridades, comprometendo a harmonização das práticas; III) insuficiência de garantias de imparcialidade processual; e IV) disparidades na aplicação transnacional do GDPR pelas NSAs, o que gera inconsistências significativas (GENTILE; LYNSKEY, 2022).

Conclui-se que o avanço normativo europeu na proteção de dados pessoais, consolidado por meio de instrumentos como a Convenção 108+ e o GDPR, reflete um compromisso com a promoção de um padrão de proteção da privacidade, tanto no âmbito interno quanto nas transferências internacionais de dados. Apesar de sua complexidade e das críticas direcionadas à aplicação transnacional do GDPR, o modelo europeu permanece uma referência global, evidenciando sua capacidade de influenciar outras jurisdições e moldar a cooperação internacional nessa matéria. Como próximo passo, será analisado o panorama da Transferência Internacional de Dados na América Latina, explorando os desafios e as oportunidades dessa região no alinhamento dos padrões de proteção de dados pessoais.

O passado colonial da América Latina, marcado por relações de poder assimétricas, ainda influencia os fluxos contemporâneos de transferência internacional de dados pessoais (FRAGOSO; MALDONADO, 2010), de modo que os países frequentemente priorizam interesses externos em detrimento da proteção efetiva dos cidadãos da região (BELLI et al., 2024; SILVA; NASCIMENTO, 2023; SILVA; NASCIMENTO, 2024; SILVA; NASCIMENTO; ROSA, 2023), confirmando-se dúvidas existentes quanto aos impactos da chegada da internet na região (GRAZZI; VERGARA, 2013).

Segundo Belli et al. (2024), embora a América Latina tenha registrado avanços em iniciativas voltadas à proteção de dados pessoais, a eficácia dessas medidas ainda é consideravelmente limitada, refletindo um desequilíbrio estrutural que perpetua a fragilidade das garantias oferecidas aos indivíduos diante de pressões globais e interesses econômicos externos.

Na América Latina, a proteção de dados pessoais encontra suas raízes na figura do *Habeas Data* (BELLI et al., 2024; RAMIRO, 2022; SILVA, 2012; GUADAMUZ, 2004), um instituto inspirado pelas Constituições da Espanha e de Portugal (MASSON, 2020; LIMBERGER, 2009). A introdução do *Habeas Data*, também conhecido como Ação de Amparo, nas constituições latino-americanas

trouxe consigo um reconhecimento implícito do Direito à Proteção de Dados, ao vinculá-lo a esse remédio constitucional (SILVA; NASCIMENTO, 2023; RAMIRO, 2022; NOUGRÈRES, 2016; SILVA, 2012). Nesse momento, houve o reconhecimento de que a instrumentalização indevida do processamento de dados deveria ser combatida para proteger as liberdades individuais, a dignidade, a democracia e a vida (NOUGRÈRES, 2016).

Conforme elucidado por Samuel Sampaio Evangelista (2021, p. 16) ‘’o discurso latinoamericano no campo tende a girar em torno do conceito de ‘’habeas data’’ em que o significado seria ‘’você deve ter os dados’’. Este conceito deriva da doutrina do devido processo legal com base no mandado de habeas corpus’’. Nesse contexto, Reginaldo Felix Nascimento (2023, p. 07), ao abordar o sistema latino-americano de proteção de dados pessoais, afirma que:

> [...] o Constitucionalismo da América Latina compreende o Direito de Proteção de Dados Pessoais. Dessa forma, é possível vislumbrar Ações Constitucionais a fim de protegê-lo. E se distingue dos sistemas Estadunidense e Europeu, visto que tais direitos na América Latina se manifestam por meio de um fenômeno de constitucionalização.

O sistema latino-americano de proteção de dados, apesar de suas particularidades formais, apresenta semelhanças materiais significativas com o modelo europeu de proteção de dados pessoais (NASCIMENTO, 2023; NOUGRÈRES, 2016; VERONESE et al., 2023a; ALBORNOZ, 2022). Isso é intensificado pela arquitetura jurídica do direito europeu que, centrada na decisão de adequação e na contratualização da sociedade internacional. Atualmente, a Europa considera países como Argentina e Uruguai como adequados em matéria de proteção de dados (BERTONI, 2020; NOUGRÈRES, 2016), o que incentiva outros países da região a também adotarem o padrão europeu (SILVA, 2012). Assim, vê-se grande inspiração dos países latino-americanos no Direito de Proteção de Dados da União Europeia (BELLI et al., 2023; NOUGRÈRES, 2016).

Conforme destacado pelo Relatório da Associação de Direitos Civis da Argentina (2016, p. 13), o processo de constitucionalização da proteção de dados na América Latina contribuiu para a criação de um arcabouço jurídico que reconhece a centralidade desse direito como pilar fundamental na promoção da privacidade e dignidade dos cidadãos da região:

> El derecho a la protección de datos tiene reconocimiento constitucional. En general, las constituciones de la región reconocen el derecho a la privacidad, pero también incluyen el llamado recurso de hábeas data, que es el derecho a la protección de los datos personales, tal el caso de las constituciones de Argentina, Brasil, Colombia, México, Perú y Venezuela.

> Pero aun cuando esta previsión no esté contenida en forma expresa en los textos constitucionales, las Cortes pertinentes han reconocido el derecho de control de la propia información.

No século XX, é possível observar a proteção de dados em sua forma embrionária. Diante disso, no século XXI, a Proteção de Dados Pessoais ganha destaque frente às novas Tecnologias de Informação e Comunicação (TICs), em meio a uma economia cada vez mais dataficada (NASCIMENTO, 2023), com um constante esvaziamento da vida social para as redes sociais (COULDRY, 2022), impulsionado por uma economia invasiva extremamente poderosa (ZUBOFF, 2015; ZUBOFF, 2021). À vista disso, conforme preceituado pela Associação de Direitos Civis da Argentina (2016, p. 34):

> Los datos personales tienen en el contexto actual un rol trascendental, provocado por los profundos cambios acontecidos en el entorno tecnológico y las transformaciones que lo anterior ha ocasionado en las prácticas de las empresas y en sus modelos de negocio, en los cambios organizacionales del Estado y en la modificación de la conducta en línea de los propios individuos. El aumento sustancial en los flujos transfronterizos motivado en la mayor integración económica y social y el mayor intercambio entre operadores públicos y privados, con más el notorio incremento de la economía digital ha generado un escenario en el que todos estos factores interactúan a tal punto que a veces se torna dificultoso establecer los límites entre ellos.

É nesse cenário que Belli et al. (2023) sugerem uma abordagem inovadora para a proteção de dados pessoais e a transferência internacional de dados na América Latina, conceituada como “tropicalismo de proteção de dados”. A perspectiva cravada visa adaptar os princípios globais de proteção de dados às especificidades culturais, econômicas e sociais da região, promovendo um modelo mais inclusivo e sensível às particularidades latino-americanas.

Diante disso, Belli et al. (2023) analisam o panorama da proteção de dados pessoais na América Latina, com foco em países como Argentina, Brasil, Colômbia, México e Uruguai. Na Argentina, os autores destacam a semelhança do ordenamento jurídico argentino com as Diretivas da União Europeia, uma vez que a legislação local só permite a transferência internacional de dados para países que apresentem legislações consideradas “adequadas” em matéria de proteção de dados. No entanto, Belli et al. (2023) fazem uma crítica tanto ao sistema argentino quanto ao europeu, apontando a falta de clareza na definição de “nível adequado de proteção”. Além disso, ressaltam que, mesmo quando o país de destino não possui proteção adequada, a transferência de dados pode ocorrer com o consentimento do titular, o que, segundo os autores, representa uma brecha significativa (BELLI et al., 2024).

No Brasil, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) regula a transferência internacional de dados, estabelecendo parâmetros que buscam alinhar o país aos padrões globais de proteção de dados (BELLI et al., 2024). Nesse sentido, grande parte das diretrizes sobre transferências internacionais foi delegada ao poder normativo da Autoridade Nacional de Proteção de Dados (ANPD), o que resultou, recentemente, na publicação da Resolução nº 19/2024, em agosto de 2024. Considerando que a proteção de dados no Brasil é abordada de maneira detalhada em um tópico específico deste documento (item 3.4), a análise aprofundada sobre a transferência internacional de dados no Brasil será realizada naquele ponto.

Por conseguinte, a Colômbia, no âmbito da transferência internacional de dados, é representada pela Superintendência de Indústria e Comércio (SIC), que busca alinhar-se aos chamados padrões “internacionais” (BELLI et al., 2024). O ordenamento jurídico colombiano, fundamentado na Lei nº 1.581/2012 e na Circular nº 05/2017, impõe restrições às transferências internacionais de dados, vinculando-as à avaliação do nível de adequação do país destinatário (BELLI et al., 2024). Embora os padrões colombianos apresentem maior rigidez, Belli et al. (2024) ressaltam que a Circular nº 05 introduziu maior flexibilidade às regras de transferência internacional de dados pessoais. Contudo, essa mesma circular foi alvo de críticas de juristas por incluir disposições que não estavam previstas expressamente na legislação, levantando questionamentos sobre sua legitimidade normativa (BELLI et al., 2024).

No México, a proteção de dados pessoais encontra fundamento no artigo 16 da Constituição Mexicana (BELLI et al., 2024; PEHLIVAN, 2021). Esse direito é regulado por dois marcos legais principais, o que o caracteriza, no México, como um modelo binário de proteção de dados (PEHLIVAN, 2021): a Lei Geral de Proteção de Dados Pessoais em Posse de Sujeitos Obrigados, que regula a atuação de entes públicos, e a Lei Geral de Proteção de Dados em Posse de Particulares, voltada para a esfera privada (BELLI et al., 2024; PEHLIVAN, 2021). Assim, a legislação mexicana abrange tanto sujeitos privados quanto públicos, estabelecendo medidas específicas para a transferência internacional de dados (BELLI et al., 2024). Destaca-se a preocupação do México com a interoperabilidade no contexto da transferência internacional de dados, refletida em acordos como o T-MEC, firmado

entre México, Estados Unidos e Canadá, que promove a integração e a proteção de dados em uma esfera transnacional (BELLI et al., 2024).

O Uruguai segue rigorosamente as normas europeias, especialmente o GDPR, refletindo uma forte influência desse padrão regulatório (BELLI et al., 2024). No país, a proteção de dados é liderada pela Unidade Reguladora e de Controle de Dados Pessoais (URCDP), que atua como a autoridade nacional responsável por essa matéria (BELLI et al., 2024). Em termos de Transferência Internacional de Dados (TID), destacam-se duas resoluções importantes: a Resolução nº 50/22/URCDP, que recomenda a adoção das cláusulas da Rede Ibero-Americana de Proteção de Dados, e a Resolução nº 41/21/URCDP, que estabelece cláusulas específicas para a transferência de dados pessoais (BELLI et al., 2024). Além disso, o Uruguai foi pioneiro entre os países não europeus ao ratificar as Convenções 108 e 108+ da União Europeia, o que reforça seu alinhamento com os padrões europeus (BELLI et al., 2024). O compromisso uruguaio foi reconhecido pela União Europeia, que considera o Uruguai como um país com nível adequado de proteção de dados pessoais, consolidando sua posição de destaque na região (BELLI et al., 2024).

De modo geral, nota-se que os países latino-americanos carecem de uma preocupação em estabelecer mecanismos de interoperabilidade regional na proteção de dados (BELLI; DONEDA, 2021; PENEDO, 2024), diferentemente de iniciativas como o T-MEC, que une Estados Unidos, México e Canadá (BELLI et al., 2024). Como afirmado por Veronese et al. (2023c), não se pode falar em uma cultura unificada de privacidade na América Latina, mas sim em uma pluralidade de concepções sobre o tema. Na Europa, a interoperabilidade é facilitada em razão do Mercado Único (PENEDO, 2024).

Nesse contexto, Belli et al. (2024) propõem que a Organização dos Estados Americanos (OEA) atue na criação de uma convenção regional sobre proteção de dados pessoais, que poderia adotar tanto a forma de *soft law* quanto de *hard law*. Contudo, surgem dois desafios cruciais: primeiramente, a presença dos Estados Unidos na OEA, cuja política de proteção de dados é notoriamente divergente dos padrões propostos, sendo um dos maiores expoentes da economia da vigilância no mundo. Em segundo lugar, a ausência de expertise técnica da OEA para abordar adequadamente as complexidades relacionadas à proteção de dados pessoais, o que poderia comprometer a eficácia de tal iniciativa.

Na América Latina, distingue-se a transferência internacional de dados da transmissão internacional de dados pessoais, sendo essa distinção fundamentada no controle e na finalidade do tratamento (ANGARITA; ZULUAGA, 2019). Conforme elucidam Angarita e Zuluaga (2019), na transferência internacional, os dados são enviados a um terceiro que, ao recebê-los, adquire autonomia para decidir sobre seu uso e tratamento. Já na transmissão internacional, os dados são direcionados a um processador que atua sob as instruções do controlador original. De forma concisa, a transferência envolve a delegação do controle sobre os dados a outra entidade, enquanto, na transmissão, delega-se apenas a execução técnica, mantendo-se a responsabilidade e o poder decisório com o controlador original (ANGARITA; ZULUAGA, 2019).

Na Colômbia, a Transmissão Internacional de Dados está definida pelo Decreto 1377 de 2013, posteriormente consolidado pelo Decreto 1074 de 2015 (ANGARITA; ZULUAGA, 2019). O artigo 24 do Decreto 1377 estabelece que o consentimento do titular dos dados pode ser dispensado caso exista um contrato de transmissão internacional de dados entre o controlador e o processador (ANGARITA; ZULUAGA, 2019). Já o artigo 25 do mesmo decreto determina que esse contrato deve obrigatoriamente prever que o processamento dos dados seja realizado sob a supervisão do controlador, definindo claramente as responsabilidades de cada parte envolvida no tratamento (ANGARITA; ZULUAGA, 2019).

No México, a Lei de Proteção de Dados Pessoais em Posse dos Particulares faz referência ao conceito de “remissão”, que possui uma equivalência ontológica com o termo “transmissão” utilizado na Colômbia (ANGARITA; ZULUAGA, 2019). De acordo com o art. 2, IX, da supramencionada lei, a remissão é definida como a comunicação de dados entre controlador e processador, seja em âmbito nacional ou internacional (ANGARITA; ZULUAGA, 2019). Assim como na regulação colombiana, essa definição mantém a responsabilidade pelo tratamento com o controlador, enquanto o processador opera de forma subordinada às instruções deste (ANGARITA; ZULUAGA, 2019).

Por outro lado, a Transferência Internacional de Dados é regulada de maneira distinta em ambos os países (ANGARITA; ZULUAGA, 2019). No México, por exemplo, o consentimento do titular é um requisito essencial para que as transferências internacionais de dados sejam realizadas (ANGARITA; ZULUAGA,

2019). Já na Colômbia, além de uma base legal específica que inclui o consentimento do titular, a transferência internacional de dados é regida pelos arts. 17 e 18 da Lei 1581 de 2012 (ANGARITA; ZULUAGA, 2019). Essas disposições são fundamentais, pois descrevem diferentes níveis de responsabilidade que se aplicam às transferências e transmissões de dados pessoais, evidenciando a necessidade de abordagens distintas para cada modalidade.

Segundo os dados levantados por Gabriel Cemin Petry e Haide Maria Hupffer (2024), dos 20 países latino-americanos, apenas 14 possuem legislação infraconstitucional específica sobre proteção de dados pessoais. Destes, 9 têm previsão expressa da proteção de dados pessoais em suas Constituições [Venezuela; Argentina, Brasil, Chile, Colômbia, Cuba, Equador, México e República Dominicana] (PETRY; HUPFFER, 2024).

Belli et al. (2024) apontam que, na América Latina, ainda não existe um instrumento de cooperação específico para a regulação da transferência internacional de dados pessoais. Assim, é preciso destacar a atuação da Rede Ibero-Americana de Proteção de Dados na América Latina, que, embora se proponha a integrar os esforços regionais e tenha incentivado discussões sobre o tema (NOUGRÈRES,2016; VERONESE et al., 2023b), segue uma orientação predominantemente europeia (BELLI et al., 2024). A Rede Ibero-Americana de Proteção de Dados tende a priorizar interesses eurocêntricos, em detrimento de um direito que poderia ser construído com base em características jurídico-ontológicas e epistemológicas específicas dos ordenamentos latino-americanos (BELLI et al., 2024) e na realidade social regional. O principal êxito reivindicado pela Rede é a implementação dos padrões europeus de proteção de dados na região, o que, apesar de representar um avanço nas discussões, levanta questionamentos sobre a autonomia regulatória e a adequação às realidades locais (BELLI et al., 2024).

A questão anterior se agrava, quando Kuner (2017) questiona a eficácia prática dos padrões de proteção de dados da União Europeia, argumentando que não há evidências concretas de que esses padrões garantam, de fato, um nível satisfatório de proteção aos dados pessoais.

Suda (2017) reforça essa crítica ao destacar a desconexão entre a perspectiva formal e abstrata da regulação da transferência internacional de dados e a realidade jurídica e econômica. Segundo Suda (2017), o debate precisa considerar

um elemento jurídico-ontológico essencial: na prática, os padrões de proteção de dados são impostos por aqueles que detêm maior representatividade no mercado, ou seja, por quem controla efetivamente as dinâmicas do mercado global. Tal concentração de poder acaba moldando as regras de proteção de dados de forma que atendam, prioritariamente, aos interesses econômicos dominantes (SILVA; NASCIMENTO, 2023).

É bastante irreal imaginar que o Brasil, com a mesma facilidade da União Europeia, poderia firmar um acordo de proteção de dados com os Estados Unidos, no qual estes aceitassem sujeitar-se a proteger os dados dos brasileiros sob o princípio de que a lei acompanha o dado. A hipótese se torna ainda mais distante diante das diferenças estruturais e de prioridades entre as políticas de proteção de dados dos dois países. Por outro lado, é perfeitamente plausível que os Estados Unidos imponham ao Brasil a recusa de aderir aos padrões brasileiros, especialmente considerando que a política de privacidade dos Estados Unidos, mais voltada para interesses econômicos e comerciais, diverge substancialmente da abordagem mais regulatória e garantista adotada pelo Brasil. A assimetria reflete as dinâmicas de poder no cenário internacional, onde o controle econômico frequentemente dita as condições de cooperação regulatória.

Se, conforme aponta Suda (2017), a influência da União Europeia na proteção de dados está intrinsecamente ligada ao seu poder econômico e à sua capacidade de moldar os mercados, isso revela, de maneira subjacente, um cenário de desequilíbrio global. Países do Sul Global, como os da América Latina, encontram-se em uma posição de desvantagem significativa, uma vez que, enquanto consumidores majoritários, enfrentam dificuldades tanto para implementar padrões robustos de proteção de dados quanto para garantir a responsabilização em caso de violações. Por exemplo, a baixa implementação de normas eficazes de proteção de dados em muitos países latino-americanos tem exposto titulares de dados pessoais a graves violações de Direitos Humanos, frequentemente ignoradas ou subestimadas no cenário global. Nesse sentido Lucas Gonçalves da Silva e Reginaldo Felix Nascimento (2023, p. 75) afirmam que:

> […] a ausência de regulação na América do Sul ofereceu solo fértil para experimentos tecnológicos em grupos vulnerabilizados, que aconteceram sem o consentimento e o conhecimento dos cidadãos envolvidos. No caso do Brasil, o projeto *Horus* da Microsoft violou o Direito à Privacidade de Crianças e Adolescentes, com foco principal na população feminina de baixa renda.

Ademais, a aplicação da jurisdição fundamentada na personalidade, que exige a implementação da lei conforme o dado, impõe condições ao país de destino, muitas vezes em detrimento de suas próprias normas internas (KUNER, 2009a).

Assim, a efetividade do direito à privacidade nas transferências internacionais de dados dependerá diretamente dos esforços realizados pelo país destinatário (KUNER, 2009a). Contudo, as autoridades de proteção de dados nesses países enfrentam enormes dificuldades para implementar medidas eficazes que assegurem tanto o direito à proteção de dados pessoais quanto o direito à privacidade (KUNER, 2009a; KUNER, 2014). Ao impor custos de transação a países externos à União Europeia, esta deveria oferecer apoio financeiro e técnico para que os padrões exigidos pudessem ser devidamente implementados (KUNER, 2014).

Em resumo, percebe-se que a proteção de dados pessoais na América Latina é um campo ainda em desenvolvimento, marcado por profundas assimetrias de poder que refletem tanto o passado colonial quanto as dinâmicas contemporâneas de influência global. Apesar de avanços normativos e do reconhecimento do *Habeas Data* como um marco jurídico regional (GUADAMUZ, 2004), a efetividade prática dessas medidas é limitada pela ausência de interoperabilidade entre os países da região, pela dependência de padrões europeus e pela falta de um instrumento regional específico que consolide uma abordagem própria. Nesse cenário, as iniciativas voltadas para a proteção de dados precisam ser fortalecidas e adaptadas às realidades locais, com atenção especial às vulnerabilidades sociais e aos riscos de exploração econômica e tecnológica. O próximo passo deste estudo será aprofundar a análise da transferência internacional de dados no contexto brasileiro.

4 EFETIVIDADE DO DIREITO À PRIVACIDADE NA TRANSFERÊNCIA INTERNACIONAL DE DADOS

4.1 TRANSFERÊNCIA INTERNACIONAL DE DADOS NO DIREITO BRASILEIRO: LEI GERAL DE PROTEÇÃO DE DADOS E O REGULAMENTO DE TRANSFERÊNCIA INTERNACIONAL DE DADOS

No art. 3º da LGPD, observa-se o escopo territorial da legislação brasileira (KRAMCSÁK, 2024). O inciso I do referido artigo estabelece que as Leis de Proteção

de Dados Pessoais Nacionais aplicam-se às operações de tratamento realizadas no território nacional.

No que concerne ao inciso III, verifica-se que a norma incide para proteger os dados pessoais objeto de tratamento, desde que tenham sido coletados no território nacional. No entanto, essa disposição merece crítica, pois a coleta de dados constitui, por si só, uma operação de tratamento, conforme a definição do inciso X do art. 5º da LGPD (ALBORNOZ, 2024). Assim, a previsão do inciso III revela-se desnecessária, uma vez que já estaria abrangida pelo inciso I, tornando-se, portanto, redundante e passível de supressão (ALBORNOZ, 2024).

Quanto ao inciso II, observa-se que ele se distingue do modelo europeu de escopo territorial (ALBORNOZ, 2024). De acordo com o inciso II do art. 3º da LGPD, esta será aplicada quando “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”.

Conforme essa previsão, a lei não considera o direcionamento (motivo) do tratamento de dados realizado fora do Brasil (ALBORNOZ, 2024). Ou seja, se o dado pertence a um titular localizado no Brasil, a LGPD deve ser aplicada (ALBORNOZ, 2024). Dito isso, enquanto o RGPD se aplica a direcionamentos voltados para o controle do comportamento dos titulares, a lei brasileira incide independentemente do direcionamento, bastando que o tratamento tenha como objeto titulares localizados no Brasil (ALBORNOZ, 2024). Nesse aspecto, o escopo territorial da legislação brasileira é mais amplo do que o da União Europeia (ALBORNOZ, 2024).

A Transferência Internacional de Dados Pessoais (TID), conforme regulada pela Lei Geral de Proteção de Dados Pessoais (LGPD), desempenha um papel essencial na discussãoo sobre proteção da privacidade e dos direitos dos indivíduos no Brasil. A LGPD estabelece um regime jurídico para a TID, buscando conciliar a necessidade de circulação global de dados com a garantia de que os direitos dos titulares sejam preservados. A seguir, será apresentada uma análise dos artigos, incisos e parágrafos que tratam especificamente da TID.

Há uma importante exceção à aplicação da lei ao tratar de dados pessoais provenientes de fora do território nacional, presente no art. 4º, inciso IV, da Lei Geral de Proteção de Dados (LGPD). De acordo com essa disposição, a LGPD não se

aplica automaticamente ao tratamento de dados de origem estrangeira, desde que esses dados não sejam objeto de comunicação, uso compartilhado ou transferência internacional para o Brasil. A regra tem como objetivo delimitar o alcance territorial da lei, restringindo sua aplicação aos casos em que os dados sejam efetivamente tratados dentro do Brasil ou estejam relacionados à interação direta com entidades brasileiras.

A segunda parte do inciso IV do art. 4º da LGPD apresenta uma condição crucial: a aplicação da lei brasileira aos dados pessoais provenientes de outros países ocorre apenas quando o país de origem desses dados não oferece um nível de proteção considerado adequado, conforme os parâmetros estabelecidos pela LGPD. O “grau de proteção adequado” exige que a legislação do país de origem assegure direitos equivalentes aos previstos na lei brasileira, garantindo proteção efetiva e suficiente.

A mencionada medida tem como objetivo evitar que dados originários de jurisdições com normas frágeis de proteção sejam transferidos para o Brasil sem que haja salvaguardas adequadas. Assim, a LGPD busca assegurar que os dados pessoais estejam protegidos de maneira uniforme, independentemente de sua origem, garantindo a manutenção dos padrões elevados de privacidade e segurança exigidos no Brasil.

Por exemplo, quando um país X não assegura níveis satisfatórios de proteção conforme os padrões da LGPD, qualquer dado pessoal originado nesse país e transferido para o Brasil deverá, obrigatoriamente, ser tratado sob as diretrizes brasileiras. Já nos casos em que o país de origem possui uma legislação robusta e equivalente à LGPD, a aplicação da lei brasileira torna-se desnecessária, uma vez que a proteção já está garantida na origem.

O art. 5º da LGPD desempenha um papel estruturante ao apresentar conceitos fundamentais que sustentam a aplicação da norma. O inciso XV aborda a transferência internacional de dados, um tema de alta relevância em um mundo cada vez mais conectado. Nele, a transferência internacional é compreendida como o envio de dados pessoais entre países ou para organismos internacionais que contem com a participação do Brasil.

A abrangência dessa definição reforça o alcance da legislação, contemplando dados processados fora do território nacional que venham a ser

enviados para o Brasil. O dispositivo demonstra a preocupação em assegurar que os dados pessoais, independentemente de sua origem geográfica, sejam protegidos de acordo com os padrões estabelecidos pela LGPD, consolidando uma resposta sólida aos desafios impostos pela globalização digital.

A conceituação da transferência internacional de dados traz implicações significativas no que tange ao controle e à proteção dos dados pessoais em sua circulação entre diferentes jurisdições. Garantir esse controle é crucial para assegurar que os direitos dos titulares sejam preservados, independentemente do local onde os dados venham a ser tratados.

A LGPD estabelece parâmetros claros para regular essas transferências, buscando evitar violações à privacidade e aos direitos fundamentais, mesmo em situações em que os dados são enviados a países cuja legislação diverge das normas brasileiras.

Quanto ao uso compartilhado de dados, o conceito do inciso XVI do art. 5º que abrange a comunicação, difusão ou interconexão de dados pessoais entre entidades distintas. Tal compartilhamento pode ocorrer entre órgãos públicos no exercício de suas funções legais, assim como entre instituições públicas e privadas, desde que devidamente autorizado. A definição também inclui o tratamento conjunto de bancos de dados pessoais por essas entidades. Refoça-se a necessidade de consentimento do titular como requisito essencial para o compartilhamento de seus dados.

A diferença entre transferência internacional de dados e uso compartilhado de dados é relevante para compreender as nuances do tratamento de dados pessoais. Enquanto a transferência internacional diz respeito ao deslocamento de dados entre países ou para organismos internacionais, o uso compartilhado está relacionado à interconexão e tratamento conjunto de dados, seja no âmbito de uma mesma jurisdição ou envolvendo diferentes jurisdições, sem necessariamente implicar o envio de dados para fora do território nacional.

Nas condições para a transferência internacional de dados pessoais, o art. 33 da LGPD assegura a proteção dos dados do titular mesmo em contextos de trânsito entre países com legislações distintas.

A primeira condição prevista no inciso I do artigo 33 da LGPD determina que a transferência internacional de dados pessoais só pode ocorrer se o país ou

organismo internacional de destino oferecer um nível de proteção compatível com os padrões estabelecidos pela lei brasileira. Portanto, cabe ao Brasil avaliar se as medidas adotadas pelo país destinatário estão em conformidade com os princípios fundamentais da LGPD, antes de autorizar a transferência.

Na segunda hipótese, prevista no inciso II do artigo 33 da LGPD, caso o país de destino não ofereça proteção equivalente à estabelecida pela LGPD, a transferência de dados poderá ocorrer se o controlador apresentar garantias adequadas de proteção. Tais garantias podem ser formalizadas por meio de cláusulas contratuais específicas, cláusulas-padrão contratuais, normas corporativas globais ou selos e certificações emitidos por autoridades competentes.

Conforme previsto no inciso III do art. 33 da LGPD, a movimentação de dados pessoais é permitida quando se faz indispensável para a cooperação jurídica internacional, especialmente em investigações criminais ou ações penais conduzidas por autoridades públicas de diferentes nações. O cumprimento de acordos de cooperação jurídica entre órgãos de distintas jurisdições fundamenta a transferência, ainda que as legislações de proteção de dados variem entre os países envolvidos. Nessa situação, a observância de obrigações legais internacionais, exigindo o compartilhamento de dados pessoais além das fronteiras nacionais.

No inciso IV do art. 33 da LGPD, permite-se a transferência de dados pessoais em casos onde seja indispensável para preservar a vida ou a integridade física do titular ou de terceiros. Trata-se de situações como atendimentos médicos de caráter urgente ou outros cenários de risco iminente, em que o compartilhamento de informações se torna vital para assegurar a proteção da vida ou a segurança física de alguém.

A transferência de dados também é possível com base no inciso V do art. 33 da LGPD, ou seja, quando há autorização expressa da Autoridade Nacional de Proteção de Dados (ANPD). Como órgão responsável pela regulamentação e fiscalização do cumprimento da LGPD, a ANPD pode conceder essa autorização em situações excepcionais, desde que as circunstâncias apresentadas justifiquem o compartilhamento de informações fora das condições padrão definidas pela legislação.

De acordo com o inciso VI do art. 33 da LGPD, a transferência de dados pessoais é permitida quando for indispensável para cumprir compromissos firmados

em acordos de cooperação internacional. A dita exceção abrange tratados ou parcerias entre países ou organizações internacionais que demandem o compartilhamento de informações pessoais, desde que as condições de proteção de dados tenham sido previamente estabelecidas e acordadas entre os participantes.

Nos termos do inciso VII do art. 33 da LGPD, a transferência de dados pessoais é admitida quando se mostra essencial para a implementação de uma política pública ou para o cumprimento de atribuições legais de um serviço público. Nessa perspectiva, o compartilhamento de informações pode ocorrer sempre que for indispensável ao desenvolvimento de políticas públicas ou ao exercício das competências conferidas a órgãos governamentais, desde que tal transferência seja realizada de forma transparente, conforme as disposições do art. 23 da LGPD.

Consoante o inciso VIII do art. 33 da LGPD, a transferência de dados pessoais é permitida quando o titular concede seu consentimento de forma específica e destacada para essa finalidade. O consentimento deve ser claro, expresso e devidamente informado, garantindo que o titular compreenda o caráter internacional da transferência e o diferencie de outras finalidades de tratamento. Essa exceção ressalta o papel fundamental do consentimento como base legítima para a movimentação de dados pessoais, desde que atendidas as exigências de transparência e especificidade.

Autoriza-se a transferência de dados pessoais quando for indispensável para atender às hipóteses previstas nos incisos II, V e VI do art. 7º da mesma lei, consoante o inciso IX do art. 33 da LGPD. Isso abrange situações em que a transferência é necessária para cumprir uma obrigação legal ou regulatória, executar um contrato, ou assegurar o exercício regular de direitos em processos judiciais, administrativos ou arbitrais.

Por último, o parágrafo único do art. 33 da LGPD complementa o disposto no inciso I, prevendo que as pessoas jurídicas de direito público, em conformidade com a Lei de Acesso à Informação (Lei nº 12.527/2011), podem solicitar à ANPD a análise do nível de proteção de dados pessoais oferecido por determinado país ou organismo internacional.

O art. 34 da Lei Geral de Proteção de Dados Pessoais (LGPD) regula a avaliação conduzida pela Autoridade Nacional de Proteção de Dados (ANPD) sobre o nível de proteção de dados pessoais em casos de transferências internacionais.

Assim, o primeiro aspecto considerado pela ANPD na avaliação prevista no inciso I do art. 34 da LGPD é o conjunto de normas gerais e setoriais vigentes no país de destino ou no organismo internacional. A mencionada previsão legal abrange o marco legal que regula a proteção de dados pessoais, englobando tanto legislações gerais quanto regulamentações específicas de setores como saúde, finanças e educação. O objetivo da avaliação é verificar se essas normas asseguram um nível de proteção compatível com os padrões da LGPD, especialmente em relação à transparência, à finalidade do tratamento e às medidas de segurança implementadas.

Outro aspecto relevante diz respeito à natureza dos dados pessoais objeto da transferência, conforme previsto no inciso II do art. 34 da LGPD. Informações sensíveis, como dados relacionados à saúde, origem étnica ou crenças religiosas, demandam uma proteção mais rigorosa devido ao maior risco de discriminação ou outras violações à privacidade do titular.

A verificação da adesão aos princípios gerais de proteção de dados pessoais e à garantia dos direitos dos titulares constitui um elemento central da análise prevista no inciso III do art. 34 da LGPD. A ANPD examinará se o país ou organismo receptor adota princípios fundamentais semelhantes aos da LGPD, como necessidade, finalidade e proporcionalidade no tratamento dos dados. Além disso, será avaliado se os titulares mantêm a possibilidade de exercer direitos essenciais, como acesso, retificação, exclusão e oposição ao tratamento, assegurando a preservação da autonomia e da privacidade dos indivíduos.

A proteção dos dados pessoais, por meio de medidas de segurança robustas, é outro aspecto crucial previsto no inciso IV do art. 34 da LGPD. A legislação exige a implementação de salvaguardas que previnam acessos não autorizados, vazamentos e outros incidentes que comprometam os dados. Nesse sentido, a ANPD analisará se o país ou organismo destinatário adota práticas alinhadas aos padrões exigidos, como o uso de criptografia, controle de acesso e outras ferramentas que garantam a integridade e a confidencialidade das informações.

Um fator relevante para a avaliação da ANPD, conforme o inciso V do art. 34 da LGPD, é a existência de garantias judiciais e institucionais no país receptor que assegurem a proteção dos direitos dos titulares. Isso envolve a presença de

mecanismos legais para reparar eventuais danos decorrentes de violações, além da atuação de autoridades independentes de proteção de dados. As supracitadas instituições devem ser capazes de fiscalizar o cumprimento das normas e assegurar a efetividade dos direitos dos indivíduos, contribuindo para uma proteção sólida.

A Resolução nº 19/2024 da ANPD estabelece os fundamentos centrais do regulamento que disciplina a transferência internacional de dados pessoais. Em um contexto globalizado, onde informações frequentemente cruzam fronteiras, a proteção de dados ganha especial relevância. A normativa busca a proteção dos direitos dos titulares, alinhando-se às diretrizes da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, que regula o tratamento de dados no Brasil.

A Resolução nº 19/2024 estabelece que a transferência de dados pessoais será permitida apenas para países ou organismos internacionais que assegurem um nível de proteção equivalente ao previsto na LGPD (inciso I do art. 1º da Resolução nº 19/2024). Em seguida, o inciso II do Art. 1º da Resolução nº 19/2024 trata das hipóteses em que a transferência internacional de dados pode ocorrer com base nas garantias oferecidas pelo controlador, ou seja, pela pessoa ou entidade responsável pelo tratamento dos dados.

No que tange aos mecanismos previstos para assegurar que as transferências internacionais de dados estejam em conformidade com a LGPD, o regulamento apresenta três alternativas. A primeira delas, descrita na alínea “a” do art. 1º, refere-se às cláusulas contratuais específicas. Essas cláusulas devem ser personalizadas para cada transferência, abordando todos os aspectos necessários para a proteção dos dados pessoais. Elas podem detalhar, por exemplo, como os dados serão tratados, quem terá acesso às informações e o período pelo qual serão armazenados. A principal vantagem desse modelo é a flexibilidade, permitindo que as cláusulas sejam adaptadas às particularidades de cada situação, garantindo operações seguras e em alinhamento com a LGPD.

A segunda opção, prevista na alínea “b” do art. 1º, é o uso de cláusulas-padrão contratuais. Esses modelos, desenvolvidos pela ANPD ou por organismos internacionais, visam assegurar que todas as partes envolvidas na transferência de dados cumpram as mesmas condições de proteção. As cláusulas-padrão são particularmente vantajosas para empresas multinacionais, pois oferecem uma

solução uniforme e prática para garantir a conformidade com a LGPD, eliminando a necessidade de negociações caso a caso.

A terceira alternativa, prevista na alínea “c” do art. 1º, é a adoção de normas corporativas globais. As regras internas, desenvolvidas por empresas ou grupos multinacionais, visam padronizar práticas de proteção de dados em todas as suas operações ao redor do mundo. Com caráter vinculativo, essas normas obrigam todas as unidades da organização a seguirem as mesmas diretrizes, independentemente da jurisdição em que estejam localizadas. Para empresas com alcance global, as normas corporativas globais representam uma solução eficiente para garantir que o tratamento de dados esteja em conformidade com a LGPD.

O parágrafo único do art. 1º da resolução esclarece que, embora o regulamento apresente essas alternativas, ele não limita a possibilidade de realizar transferências internacionais de dados com base em outros mecanismos previstos diretamente na LGPD, especialmente no art. 33. À vista disso, percebe-se situações em que a transferência é permitida sem a necessidade de regulamentação adicional, como nos casos de consentimento explícito do titular ou para a execução de acordos internacionais.

No art. 2º da Resolução nº 19/2024 da ANPD, observar-se-á diretrizes fundamentais para a transferência internacional de dados pessoais, alinhadas à Lei Geral de Proteção de Dados (LGPD) e ao regulamento da ANPD. O primeiro inciso assegura que os dados pessoais transferidos para fora do país devem permanecer sob o mesmo nível de proteção exigido pela LGPD, independentemente de sua localização. Quanto ao segundo, enfatiza-se a relevância de adotar procedimentos simples e interoperáveis para a transferência internacional de dados. Por sua vez, o terceiro inciso incentiva o livre fluxo transfronteiriço de dados, promovendo uma movimentação eficiente entre países. Ao tratar da responsabilização das organizações envolvidas na transferência de dados, o quarto inciso exige que implementem medidas efetivas para demonstrar o cumprimento da LGPD. É importante, ainda, a transparência nas operações de transferência de dados, conforme previsão do quinto inciso. *In fine*, o sexto inciso reforça a necessidade de implementar boas práticas de segurança no tratamento de dados pessoais.

No regulamento, vê-se definições cruciais, no art. 3º, para esclarecer os conceitos relacionados às operações de transferência internacional de dados

pessoais. Esses termos fornecem a base para compreender como as informações devem ser tratadas em conformidade com a LGPD e o regulamento da ANPD.

O conceito de exportador, descrito no inciso I, identifica o agente de tratamento, situado no Brasil ou no exterior, responsável pela transferência de dados pessoais a outro agente, chamado importador. O exportador pode ser uma pessoa física ou jurídica. Mencionado no inciso II, o importador é o agente que recebe os dados pessoais enviados pelo exportador. Tal agente pode estar situado em outro país ou ser um organismo internacional.

A transferência, descrita no inciso III, consiste em qualquer operação na qual um agente de tratamento, conhecido como exportador, transmite, compartilha ou disponibiliza dados pessoais para outro agente, denominado importador. A transferência internacional de dados, conforme definida no inciso IV, é o processo de enviar dados pessoais para países estrangeiros ou organismos internacionais. A coleta internacional de dados, mencionada no inciso V, refere-se à coleta direta de dados pessoais realizada por um agente de tratamento situado fora do Brasil. Diferentemente da transferência, que implica a movimentação de dados de uma entidade para outra, a coleta diz respeito à obtenção de dados diretamente do titular.

No inciso VI, a definição de grupo ou conglomerado de empresas descreve um conjunto de empresas com personalidades jurídicas próprias, mas sob controle comum, que operam de maneira integrada.

No caso do responsável pela entidade (inciso VII), observa-se que este é a sociedade empresarial com sede no Brasil que se responsabiliza por qualquer violação das normas globais de proteção de dados, mesmo que a falha tenha ocorrido em uma empresa pertencente ao grupo no exterior.

Os métodos legais que autorizam a transferência de dados entre países são chamados de mecanismos de transferência internacional de dados. Com base no incio VIII, tais mecanismos incluem garantias de adequação, consentimento do titular ou cláusulas contratuais específicas, entre outros.

A definição dos organismos internacionais encontra-se no inciso IX, que são organizações regidas pelo direito internacional público, formadas por acordos entre dois ou mais países.

De acordo com o inciso X aborda, as medidas de segurança são conceituadas como ações técnicas e administrativas adotadas para proteger os dados pessoais contra acessos não autorizados, destruição, perda, ou alterações.

As responsabilidades para o controlador na realização da transferência internacional de dados pessoais está definida no art. 4º do Capítulo III da Resolução nº 19/2024 da ANPD. O controlador deve verificar, conforme as disposições da Lei nº 13.709/2018 (LGPD) e do Regulamento, se a operação de tratamento de dados realmente caracteriza uma transferência internacional (inciso I). Além disso, o controlador precisa garantir que a operação esteja em conformidade com a legislação brasileira de proteção de dados (inciso II) e que seja respaldada por uma base legal válida (inciso III), como as previstas no regulamento, para a transferência internacional.

O § 1º do artigo estabelece que o operador, que auxilia o controlador, deve fornecer todas as informações relevantes para garantir que as exigências do artigo sejam atendidas. Ou seja, o operador tem a obrigação de colaborar ativamente, fornecendo dados ou informações que possam ser necessários para a conformidade do processo. Já o § 2º destaca a importância de que tanto o controlador quanto o operador adotem medidas adequadas para assegurar que as normas de proteção de dados sejam respeitadas.

Exposta no art. 5º da Resolução nº 19/2024 da ANPD, vê-se a hipótese de caracterização da transferência internacional de dados pessoais. De acordo com o texto, a transferência será caracterizada sempre que o exportador (o agente de tratamento de dados localizado no Brasil ou em outro país) enviar dados pessoais para o importador, seja ele também um agente de tratamento ou um organismo internacional, localizado em outro país. Ou seja, a transferência é uma ação ativa onde os dados deixam a jurisdição do exportador e chegam ao importador, configurando a transferência internacional.

Por outro lado, o art. 6º esclarece que a coleta internacional de dados não se enquadra como uma transferência internacional. A coleta refere-se ao ato de um agente de tratamento, localizado no exterior, coletando dados diretamente de indivíduos (titulares) em um país diferente. Esse processo não envolve a movimentação de dados de uma jurisdição para outra, sendo, portanto, segundo o regulamento, distinto da transferência internacional de dados.

O parágrafo único do art. 6º especifica que, embora a coleta internacional não seja considerada uma transferência, ela ainda deve seguir as normas estabelecidas pela Lei nº 13.709/2018 (LGPD). Assim, se a coleta ocorrer em uma das situações previstas no art. 3º da LGPD, como o consentimento explícito do titular ou a necessidade para a execução de um contrato, as disposições da Lei deverão ser observadas para garantir a proteção dos dados pessoais.

Os requisitos que a transferência internacional de dados pessoais deve atender estão previstos no art. 7º da Resolução nº 19/2024 da ANPD. À vista disso, o primeiro inciso afirma que a transferência internacional de dados precisa observar a legislação brasileira quando a operação de tratamento de dados ocorrer dentro do território nacional. Infere-se que, mesmo que os dados sejam transferidos para fora do Brasil, se a operação inicial do tratamento ocorrer dentro do território nacional, ela estará sujeita à LGPD e às disposições do regulamento. O inciso também ressalva o disposto no inciso IV do art. 4º da LGPD, que trata das exceções à aplicação da lei, e menciona que o disposto no art. 8º do regulamento também precisa ser observado. O art. 8º trata da aplicação da LGPD aos dados provenientes de fora do Brasil, esclarecendo como a lei se aplica quando os dados são coletados fora do país, mas tratados em território nacional.

As situações em que a transferência internacional de dados deve obedecer à legislação nacional, quando a atividade de tratamento tiver como objetivo a oferta ou fornecimento de bens ou serviços a indivíduos localizados no território nacional, ou quando os dados de pessoas localizadas no Brasil forem tratados, independentemente de onde o tratamento ocorra, são discutidas no inciso II. Ou seja, se uma empresa ou entidade que esteja localizada fora do Brasil realizar operações de tratamento de dados de pessoas localizadas no Brasil, ela estará sujeita às disposições da LGPD.

A transferência internacional de dados, segundo o inciso III, também deve seguir as disposições da LGPD quando os dados pessoais, que serão objeto do tratamento, forem coletados no território nacional. Assim, se os dados forem coletados em território brasileiro, a legislação brasileira se aplica independentemente de onde os dados são posteriormente tratados ou para onde são transferidos.

O parágrafo único do art. 7º esclarece que aplicação da legislação nacional à transferência internacional de dados não depende do meio utilizado para a

realização da transferência, nem do país em que os agentes de tratamento estão localizados, ou de onde os dados estão armazenados. Assim, pode-se concluir que, independentemente de como os dados sejam transferidos (seja por via digital, física, etc.), ou do local em que a empresa que trata os dados esteja estabelecida, a LGPD continuará a se aplicar.

No art. 8º da Resolução nº 19/2024 da ANPD, a aplicação da Lei Geral de Proteção de Dados (LGPD) em relação aos dados pessoais provenientes do exterior. Ele estabelece que, sempre que esses dados forem tratados no Brasil, a LGPD será aplicável.

Nesse ínterim, parágrafo 1º traz exceções à aplicação da LGPD aos dados pessoais que provêm do exterior. As citadas exceções ocorrem em duas situações específica. No inciso I, a LGPD não se aplica quando ocorre o trânsito de dados pessoais para fora do Brasil, sem que haja comunicação ou uso compartilhado de dados com agentes de tratamento localizados no Brasil. Ou seja, se os dados são movimentados para fora do território nacional sem qualquer tipo de interação com agentes no Brasil, a LGPD não será invocada para regular essa operação. No inciso II, também há uma exceção quando os dados, previamente tratados no Brasil, são retornados ao país ou organismo internacional de origem. Nesse caso, a LGPD não se aplica se o país ou organismo internacional de origem oferecer um grau de proteção de dados adequado, reconhecido por uma decisão formal da Autoridade Nacional de Proteção de Dados (ANPD).

O parágrafo segundo reforça a incidência da LGPD no caso de transferências internacionais, mesmo quando a ANPD emita uma decisão de adequação, caso isso coloque em risco os direitos dos titulares ou os princípios da proteção de dados pessoais. Em outras palavras, a decisão da ANPD não poderá ser usada para evitar a aplicação da LGPD se houver risco de violação dos direitos dos titulares.

Finalmente, o parágrafo 3º esclarece que a não aplicação da LGPD, conforme as exceções previstas, não isenta o cumprimento de outras leis ou regulamentos que tratem da inviolabilidade e sigilo das comunicações, das medidas técnicas e de segurança e do acesso a dados por autoridades públicas. Isto é, mesmo quando a LGPD não se aplica diretamente, outras normativas ou legislações, especialmente aquelas que tratam de segurança de dados e da proteção de informações sensíveis,

ainda devem ser seguidas, independentemente da situação de adequação da proteção de dados.

O art. 9º da Resolução nº 19/2024 da ANPD estabelece as condições para a transferência internacional de dados pessoais, visando assegurar que esse processo seja realizado de maneira legítima, transparente e conforme as finalidades informadas ao titular. A transferência só poderá ocorrer quando atender a propósitos legítimos, específicos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com as finalidades originais.

No inciso I do art. 9º, observa-se que a transferência internacional de dados deve ser fundamentada em uma das hipóteses legais descritas nos artigos 7º ou 11 da LGPD. Nesse aspecto, o artigo 7º trata das bases legais para o tratamento de dados pessoais, como o consentimento do titular ou a necessidade de cumprimento de obrigação legal, enquanto o artigo 11 aborda o tratamento de dados sensíveis.

Em continuidade, o inciso II descreve os mecanismos válidos para a realização da transferência internacional de dados. A primeira opção prevista é a transferência para países ou organismos internacionais que garantam um nível de proteção de dados equivalente ao exigido pela LGPD, reconhecido por meio de decisão de adequação emitida pela ANPD. Com isso, entende-se que, para a transferência ser permitida, o país ou organismo de destino deve ter uma legislação de proteção de dados semelhante à brasileira.

A segunda opção são as cláusulas-padrão contratuais, normas corporativas globais ou cláusulas contratuais específicas. A terceira alternativa são as hipóteses previstas nos incisos II, “d”, e III a IX do artigo 33 da LGPD, que incluem, entre outras, situações de necessidade de cumprimento de contrato, proteção da vida do titular ou quando houver consentimento explícito do titular para a transferência.

A partir do princípio da minimização de dados, conforme preconizado no parágrafo único do art. 9º, determina-se que a transferência internacional de dados deve se limitar ao mínimo necessário para cumprir com a finalidade estabelecida. Os dados transferidos devem ser pertinentes, proporcionais e não excessivos em relação aos objetivos do tratamento.

De acordo com o art. 10 da Resolução nº 19/2024 da ANPD, é possível que a Autoridade Nacional de Proteção de Dados (ANPD) emita uma decisão de adequação, reconhecendo a equivalência do nível de proteção de dados pessoais de

um país estrangeiro ou organismo internacional com a legislação nacional brasileira, estabelecida pela Lei nº 13.709/2018 (LGPD) e pelo próprio regulamento. A decisão de adequação é um mecanismo que permite a transferência internacional de dados pessoais para países ou organismos que atendam a requisitos de proteção de dados similares aos exigidos pela LGPD.

Assim, o art. 11 da Resolução nº 19/2024 da ANPD estabelece os critérios que devem ser seguidos para avaliar o nível de proteção de dados pessoais de países estrangeiros ou organismos internacionais. Os critérios são fundamentais para garantir que as transferências internacionais de dados ocorram de forma segura e em conformidade com a Lei nº 13.709/2018 (LGPD).

Dito isso, o inciso I destaca a importância das normas gerais e setoriais em vigor no país de destino ou organismo internacional, que devem ter impacto direto sobre a proteção de dados pessoais. O apontado critério se concentra na avaliação da legislação do país ou organismo internacional quanto à proteção dos dados, considerando as leis específicas que regem o tratamento de dados pessoais. A partir dessa análise, verifica-se se essas normas oferecem a mesma segurança que a legislação nacional. O inciso II foca na natureza dos dados. Aqui, o critério avalia o tipo de dado que será transferido, pois diferentes tipos de dados podem exigir níveis de proteção diferentes, dependendo da sensibilidade das informações. Isso implica que dados mais sensíveis, como dados de saúde ou dados financeiros, exigem um nível de proteção mais rigoroso. O inciso III trata da observância dos princípios gerais de proteção de dados pessoais e dos direitos dos titulares, conforme previsto pela LGPD. No inciso IV, o regulamento exige que sejam adotadas medidas de segurança adequadas para minimizar os impactos sobre as liberdades civis e os direitos fundamentais dos titulares. O inciso V destaca a necessidade de garantias judiciais e institucionais que assegurem o respeito aos direitos de proteção de dados pessoais. A análise de garantias judiciais envolve verificar se existe um sistema legal funcional que permita ao titular dos dados buscar reparação ou responsabilizar os responsáveis pelo tratamento indevido dos seus dados. Já as garantias institucionais se referem à existência de órgãos ou entidades responsáveis por monitorar e garantir o cumprimento das normas de proteção de dados.

Por fim, o inciso VI considera outras circunstâncias específicas relativas à transferência. Este critério oferece uma flexibilidade para avaliar aspectos adicionais

que possam influenciar a transferência de dados, como acordos internacionais, políticas específicas do setor ou outras variáveis relevantes.

Os parágrafos que seguem detalham como esses critérios devem ser avaliados. O § 1º esclarece que a avaliação das normas mencionadas no inciso I se limita àquelas que são diretamente aplicáveis ou que gerem impactos significativos sobre o tratamento de dados. Consequentemente, não basta olhar para qualquer legislação; é necessário analisar as que afetam especificamente a proteção de dados pessoais.

A avaliação da legislação local deve verificar, com espeque no § 2º, se os agentes de tratamento no país de destino têm obrigações claras para implementar medidas de segurança adequadas, considerando a natureza dos dados e os riscos envolvidos. Ou seja, o critério foca na responsabilidade das entidades que lidam com os dados e na eficácia das medidas de segurança adotadas. Ademais, o § 3º, por sua vez, destaca a relevância de um órgão regulador independente no país de destino, que tenha a competência para garantir o cumprimento das normas de proteção de dados e os direitos dos titulares.

Prevista no art. 12 da Resolução nº 19/2024 da ANPD, a avaliação do nível de proteção de dados pessoais, leva em conta não apenas a legislação do país de destino, mas também outros fatores relevantes que influenciam a transferência de dados. No inciso I, a avaliação considera os riscos e benefícios decorrentes da decisão de adequação, analisando a garantia dos princípios e direitos do titular dos dados, assim como o regime de proteção estabelecido pela Lei nº 13.709/2018 (LGPD). O risco e o benefício são ponderados de forma a assegurar que a transferência de dados não comprometa a proteção dos direitos dos indivíduos, mesmo quando os dados saem da jurisdição brasileira.

Já no inciso II, percebe-se um foco nos impactos da decisão sobre o fluxo internacional de dados. Isso inclui as implicações para as relações diplomáticas entre os países envolvidos, o comércio internacional e a cooperação internacional entre o Brasil e outros países ou organismos internacionais. A avaliação leva em consideração a influência que a decisão pode ter nas relações globais e nas trocas comerciais.

O parágrafo único traz um ponto importante: ele determina que a ANPD dará prioridade à avaliação do nível de proteção de dados de países ou organismos

internacionais que ofereçam tratamento recíproco ao Brasil. Assim, países que, ao reconhecerem a adequação das práticas de proteção de dados do Brasil, também garantam um nível semelhante de proteção para dados brasileiros em seu território.

O art. 13 da Resolução nº 19/2024 da ANPD trata do procedimento para a emissão de uma decisão de adequação, que consiste no reconhecimento pela ANPD de que o nível de proteção de dados pessoais em um determinado país ou organismo internacional é equivalente ao previsto pela Lei nº 13.709/2018 (LGPD).

No inciso I, o procedimento para iniciar a decisão de adequação pode ser instado por uma decisão do Conselho Diretor da ANPD, ou então por solicitação das pessoas jurídicas de direito público mencionadas no parágrafo único do art. 1º da Lei nº 12.527/2011. A solicitação pode ser feita por entidades públicas que possuem competências relacionadas à proteção de dados, permitindo que a ANPD avalie o nível de proteção de dados de outros países ou organismos internacionais.

A área técnica competente da ANPD será responsável por instruir o procedimento, seguindo o que é estipulado pelo Regimento Interno da ANPD, de acordo com o inciso II. Após analisar a solicitação, a área técnica emitirá uma manifestação sobre o mérito da decisão de adequação. Caso necessário, a área técnica indicará as condicionantes que devem ser observadas para garantir que o nível de proteção de dados esteja em conformidade com os requisitos exigidos pela legislação brasileira.

No inciso III, é determinado que, após a manifestação da Procuradoria Federal Especializada, o procedimento será levado para a deliberação final do Conselho Diretor da ANPD, conforme o processo estabelecido pelo Regimento Interno da ANPD. A Procuradoria Federal Especializada revisa a legalidade e os aspectos jurídicos da decisão antes que o Conselho Diretor tome a decisão final.

O parágrafo 1º destaca que órgãos e entidades da Administração Pública com competências relacionadas ao tema poderão ser informados sobre o início do processo e terão a opção de apresentar manifestações, conforme suas competências legais. Isso assegura que outras partes interessadas possam contribuir com informações relevantes antes da decisão final da ANPD.

A decisão de adequação será formalizada por meio de uma Resolução do Conselho Diretor da ANPD e será publicada na página da ANPD na internet, tornando o processo transparente e acessível ao público (parágrafo 2º).

O procedimento que deve ser seguido quando o processo envolve a elaboração de documentos, fornecimento de informações ou outros atos relacionados ao reconhecimento do Brasil como um país com nível de proteção adequado, por outro país ou organismo internacional, é descrito pelo art. 14. Este processo seguirá os mesmos procedimentos descritos no art. 13.

Já no art. 15 da Resolução nº 19/2024 da ANPD observa-se cláusulas-padrão contratuais, que são um conjunto de disposições contratuais elaboradas e aprovadas pela ANPD, conforme descrito no Anexo II do regulamento. As cláusulas-padrão contratuais são baseadas no inciso II, alínea “b”, do art. 33 da LGPD, que trata das condições sob as quais os dados pessoais podem ser transferidos para fora do Brasil.

As cláusulas-padrão oferecem uma solução prática e padronizada para as empresas que necessitam realizar transferências internacionais de dados, permitindo que as transferências sejam feitas de forma mais eficiente.

O art. 16 da Resolução nº 19/2024 da ANPD trata da validade das transferências internacionais de dados que são realizadas com base nas cláusulas-padrão contratuais, previstas no Anexo II do regulamento. A principal condição para que a transferência seja considerada válida é que as cláusulas-padrão sejam adotadas de forma integral, sem qualquer modificação, e que sejam incluídas em um instrumento contratual formalizado entre o exportador (quem envia os dados) e o importador (quem recebe os dados).

As cláusulas-padrão podem ser incorporadas em diferentes tipos de contratos (§ 1º do art 16). Tais cláusulas podem ser parte de um contrato específico para regulamentar as transferências internacionais de dados, ou seja, um contrato que tenha como único objetivo estabelecer as condições para a transferência de dados entre as partes (inciso I). No II, amplia-se essa possibilidade, permitindo que as cláusulas-padrão sejam adicionadas a um contrato mais amplo, que trate de outras questões além da transferência de dados. Nesse caso, o contrato precisa ser formalizado por meio de um termo aditivo, assinado tanto pelo exportador quanto pelo importador, para garantir que as cláusulas-padrão sejam cumpridas dentro do contexto do contrato original.

Quanto as disposições contidas em outros termos do contrato ou em contratos relacionados não podem alterar ou contrariar as cláusulas-padrão (§ 2º),

qualquer outra condição prevista no contrato que seja incompatível com as cláusulas-padrão, ou que tente modificá-las, será considerada inválida.

Caso as cláusulas-padrão sejam integradas em um contrato mais amplo, como no caso do inciso II do § 1º, as Seções I, II e III do Anexo II do regulamento devem ser anexadas ao contrato como um documento separado (§ 3º). Isso visa garantir que as cláusulas-padrão, que contêm regras específicas e obrigatórias para a transferência de dados, sejam facilmente acessíveis e cumpridas pelas partes envolvidas na transferência internacional de dados.

O art. 17 da Resolução nº 19/2024 da ANPD aborda as medidas de transparência que o controlador deve adotar ao realizar transferências internacionais de dados pessoais. As supracitadas medidas visam garantir que os titulares de dados estejam bem informados sobre o processo de transferência e sobre como seus dados são tratados. O dispositivo estabelece que, caso solicitado, o controlador deverá fornecer ao titular a íntegra das cláusulas contratuais utilizadas na transferência internacional de dados. No entanto, o controlador deve observar os segredos comerciais e industriais, ou seja, informações sensíveis que não podem ser divulgadas por questões de proteção da competitividade ou outros interesses comerciais legítimos.

Dito isso, o controlador deve atender a essa solicitação dentro de um prazo de 15 dias (§ 1º). Caso haja um prazo diferente estabelecido em regulamentação específica da ANPD, ele deverá ser seguido.

Assim, o regulamento exige que o controlador também publique um documento em sua página na Internet com informações detalhadas sobre a transferência internacional de dados (§ 2º). Tal documento deve ser redigido em português, utilizando uma linguagem simples, clara e precisa, para garantir que qualquer titular de dados possa compreendê-lo.

Há, ainda, o processo pelo qual a Autoridade Nacional de Proteção de Dados (ANPD) pode reconhecer a equivalência de cláusulas-padrão contratuais de outros países ou organismos internacionais com as cláusulas previstas no Anexo II do regulamento (art. 18 da Resolução nº 19/2024).

À vista disso, o § 1º detalha os passos do procedimento para reconhecimento de equivalência. O processo pode ser iniciado pelo Conselho Diretor da ANPD, seja de ofício ou por solicitação de partes interessadas. Após a solicitação, a área técnica

competente da ANPD será responsável por avaliar a proposta de equivalência, e, se necessário, indicará as condicionantes a serem seguidas. A manifestação da Procuradoria Federal Especializada também será requerida antes da deliberação final do Conselho Diretor.

Durante esse procedimento, o Conselho Diretor da ANPD pode decidir realizar uma consulta pública à sociedade, permitindo que outras partes interessadas possam se manifestar sobre a proposta de equivalência (§ 2º).

Órgãos e entidades da Administração Pública que tenham competências relacionadas à proteção de dados possam ser notificados sobre o processo e têm a faculdade de apresentar suas manifestações, dentro de suas atribuições legais (§ 3º). Dito isso, o requerimento de reconhecimento de equivalência de cláusulas-padrão contratuais deve ser acompanhado por documentos e informações detalhadas, como o texto completo das cláusulas-padrão contratuais traduzido para o português, a legislação aplicável e outros documentos pertinentes, incluindo guias e orientações da autoridade de proteção de dados relevante (§ 4º). Também é necessário apresentar uma análise comparativa entre as cláusulas nacionais e as propostas para garantir que as cláusulas estrangeiras atendem aos requisitos da LGPD e do regulamento da ANPD.

Os critérios que a Autoridade Nacional de Proteção de Dados (ANPD) deve considerar ao decidir sobre a proposta de equivalência de cláusulas-padrão contratuais estão previstos no art. 19 da Resolução nº 19/2024 da ANPD. Os critérios visam assegurar que as cláusulas de outros países ou organismos internacionais atendam aos mesmos padrões de proteção de dados exigidos pela Lei Geral de Proteção de Dados (LGPD) e pelo regulamento da ANPD.

A decisão da ANPD sobre a equivalência das cláusulas-padrão contratuais deverá avaliar se essas cláusulas são compatíveis com as disposições da LGPD e do regulamento da ANPD (inciso I). O inciso II expande a análise ao considerar os riscos e benefícios decorrentes da aprovação das cláusulas-padrão contratuais equivalentes. O parágrafo único reforça que, ao tomar sua decisão, a ANPD priorizará a aprovação de cláusulas-padrão contratuais que possam ser utilizadas por outros agentes de tratamento em situações similares de transferência internacional de dados.

O art. 20 da Resolução nº 19/2024 da ANPD estabelece o procedimento final para a aprovação das cláusulas-padrão contratuais reconhecidas como equivalentes. Quando a ANPD concluir que as cláusulas-padrão contratuais de um país ou organismo internacional são equivalentes às cláusulas-padrão contratuais brasileiras, a decisão será formalizada através de uma Resolução do Conselho Diretor.

O parágrafo único do artigo especifica que as cláusulas-padrão contratuais reconhecidas como equivalentes são consideradas um mecanismo válido para realizar transferências internacionais de dados pessoais. A dita validade está em conformidade com o art. 33, inciso II, alínea “b”, da Lei nº 13.709/2018 (LGPD), que permite a transferência de dados com base em garantias adequadas de proteção.

A possibilidade de o controlador solicitar a aprovação de cláusulas contratuais específicas para realizar a transferência internacional de dados pessoais podem ser vistas no art. 21 da Resolução nº 19/2024 da ANPD. As cláusulas contratuais específicas só serão aprovadas quando o controlador não puder usar as cláusulas-padrão contratuais, que são mais comuns e amplamente aplicáveis (§1º). A exceção se dá quando há circunstâncias excepcionais, que podem ser de fato ou de direito, e que precisam ser adequadamente comprovadas pelo controlador. Ou seja, se as cláusulas-padrão não forem viáveis ou não atenderem ao caso específico, o controlador pode recorrer às cláusulas específicas, desde que justifique a necessidade de uma solução personalizada.

Mesmo no caso das cláusulas contratuais específicas, a legislação nacional de proteção de dados pessoais (a LGPD) deve ser observada (§2º). Além disso, essas cláusulas estarão sujeitas à fiscalização da ANPD, garantindo que, apesar da flexibilidade oferecida por essas cláusulas, o cumprimento das normas de proteção de dados seja monitorado e garantido pela autoridade reguladora.

O art. 22 da Resolução nº 19/2024 da ANPD trata da necessidade de o controlador submeter à ANPD a íntegra das cláusulas que regerão a transferência internacional de dados pessoais, incluindo as cláusulas específicas. Em consequência, o controlador deve enviar as cláusulas contratuais que detalham como os dados serão tratados, com o objetivo de garantir que essas cláusulas estejam em conformidade com a Lei nº 13.709/2018 (LGPD) e o regulamento da ANPD.

Ao conceber essas cláusulas, a ANPD considerará alguns aspectos importantes para avaliar a conformidade das cláusulas específicas (§1º). A ANPD verificará se as cláusulas são compatíveis com a LGPD e com o regulamento da ANPD, além de garantir que elas ofereçam um nível de proteção de dados equivalente ao das cláusulas-padrão contratuais nacionais (inciso I).

No inciso II, o regulamento também exige que a ANPD considere os riscos e benefícios associados à aprovação das cláusulas específicas. Entre os pontos que devem ser avaliados, está a garantia dos direitos dos titulares de dados e o cumprimento do regime de proteção de dados previstos pela LGPD. Além disso, a ANPD precisa analisar os impactos da transferência internacional de dados no fluxo de informações entre os países, nas relações diplomáticas, no comércio internacional e na cooperação entre o Brasil e outros países ou organismos internacionais.

Quando se trata da aprovação de cláusulas específicas, a ANPD dará prioridade àquelas cláusulas que possam ser aplicadas por outros agentes de tratamento em circunstâncias semelhantes (§2º). Pode-se interpretar que, para facilitar a padronização e a implementação de práticas de proteção de dados, a ANPD buscará que as cláusulas específicas sejam aplicáveis de forma mais ampla, beneficiando a transferência de dados em diferentes contextos e entre diferentes organizações.

O art. 23 da Resolução nº 19/2024 da ANPD estabelece requisitos importantes para a submissão das cláusulas contratuais à aprovação da ANPD. O controlador, sempre que possível, deve adotar as cláusulas-padrão contratuais (inciso I). Isso é importante, pois as cláusulas-padrão oferecem uma base uniforme para a transferência internacional de dados, garantindo que todas as partes envolvidas sigam as mesmas condições de proteção.

Exige-se que, caso o controlador adote cláusulas específicas, ele deve indicar claramente quais são essas cláusulas e justificar sua adoção, conforme os termos estabelecidos no art. 22, II, do regulamento.

O art. 24 complementa ao afirmar que as cláusulas contratuais específicas, como mencionado no art. 23, devem ser submetidas à aprovação da ANPD, seguindo o processo descrito no Capítulo VIII da resolução. Isso implica que as cláusulas não podem ser adotadas sem a validação prévia da ANPD, garantindo que

elas atendam aos padrões e exigências de proteção de dados estabelecidos pela LGPD e pela própria ANPD.

As Normas Corporativas Globais (NCG), que foram inseridas na Lei Geral de Proteção de Dados do Brasil com fundamento nas *Binding Corporate Rules* (BCR) do modelo europeu, permitiram a ocorrência de transferência de dados entre empresas do mesmo grupo, que juntas, uniformizam uma política interna deproteção de dados (BELLI et al., 2024).

É no art. 25 da Resolução nº 19/2024 da ANPD que se observa a hipótese de transferência através das normas corporativas globais, como sendo um mecanismo específico para as transferências internacionais de dados pessoais dentro de grupos ou conglomerados de empresas. As normas são estabelecidas para regulamentar como os dados pessoais podem ser transferidos entre as organizações que fazem parte do mesmo grupo empresarial, independentemente das fronteiras nacionais. A principal característica das normas corporativas globais é que elas possuem um caráter vinculante para os membros do grupo que as subscreverem, ou seja, todas as empresas ou entidades que fazem parte do conglomerado e concordam com a norma devem segui-la, garantindo que a transferência de dados pessoais entre elas esteja em conformidade com as disposições legais.

O parágrafo único do artigo reforça que as normas corporativas globais só são válidas para realizar transferências internacionais de dados pessoais dentro das organizações ou países que estão abrangidos por essas normas. Em outras palavras, a abrangência da norma se limita aos membros do grupo empresarial ou aos países onde o grupo tem atuação, garantindo que a transferência de dados esteja restrita a esse contexto específico e que todos os envolvidos cumpram as diretrizes estabelecidas pela norma.

O art. 26 da Resolução nº 19/2024 da ANPD estabelece que as normas corporativas globais devem estar vinculadas à implementação de um programa de governança, que cumpra as condições mínimas estabelecidas no § 2º do art. 50 da Lei nº 13.709, de 14 de agosto de 2018 (LGPD).

Há uma série de requisitos que devem ser atendidos pelas normas corporativas globais para que estas possam ser válidas para a transferência internacional de dados no art. 27 da Resolução nº 19/2024 da ANPD.

O inciso I exige que as normas corporativas globais descrevam as transferências internacionais de dados, incluindo as categorias de dados pessoais, as operações de tratamento realizadas, as finalidades dessas operações, a base legal para a transferência e os tipos de titulares de dados envolvidos. Ademais, o inciso II exige a identificação dos países para os quais os dados podem ser transferidos, assegurando que as organizações tenham um entendimento de onde os dados estão sendo enviados e se os destinos estão sujeitos a níveis adequados de proteção.

Exige-se a descrição da estrutura do grupo ou conglomerado de empresas, incluindo a identificação das entidades vinculadas, os papéis desempenhados por cada uma delas no tratamento de dados e os dados de contato das organizações responsáveis por tratar os dados pessoais (inciso III). Isso facilita a transparência e a responsabilidade, já que todas as entidades envolvidas ficam identificadas.

As normas corporativas globais devem ser vinculantes para todos os membros do grupo ou conglomerado de empresas que as subscreverem, incluindo seus funcionários (inciso IV). É necessário de delimitar as responsabilidades pelo tratamento dos dados, identificando qual entidade será responsável por cumprir as obrigações de proteção de dados (inciso V).

As normas devem indicar os direitos dos titulares de dados, como o acesso, a retificação, a exclusão e o direito de peticionar contra o controlador perante a ANPD (inciso VI). Além disso, deve ser indicado um canal de fácil acesso para o exercício desses direitos.

Deve-se-á prever regras para a revisão das normas corporativas globais, incluindo a previsão de sua submissão à prévia aprovação da ANPD, garantindo que as normas permaneçam atualizadas e em conformidade com a legislação (inciso VII).

A norma corporativa global tem que prever comunicação imediata à ANPD caso ocorra uma alteração que afete a observância dos princípios de proteção de dados, especialmente quando um dos membros do grupo estiver sujeito a uma legislação de outro país que dificulte o cumprimento dessas normas (inciso VIII).

O art. 28 da Resolução nº 19/2024 da ANPD estabelece que as normas corporativas globais devem ser submetidas à aprovação da Autoridade Nacional de Proteção de Dados (ANPD). Essa aprovação segue o processo descrito no Capítulo

VIII da resolução, que trata das disposições gerais e procedimentos relacionados à validação e conformidade das normas corporativas globais com a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD), bem como com as demais regulamentações pertinentes.

Em conclusão, a estrutura regulatória compreendida pela Lei Geral de Proteção de Dados (LGPD) e pela Resolução nº 19/2024 da ANPD procura estabelecer um conjunto de diretrizes com compromisso de governar a transferência internacional de dados pessoais. Estes instrumentos normativos visam adequar o tratamento de dados pessoais às exigências de mercado. As regulações tentam impor requisitos específicos para garantir que os dados pessoais transferidos internacionalmente tentem manter um nível de proteção consistente com os padrões estabelecidos nacionalmente, com a perspectiva de, assim, preservar os direitos dos indivíduos em um contexto globalizado.

4.2 COMPREENSÃO CRÍTICA DA REGULAÇÃO VIGENTE

A Resolução nº 19/2024 da ANPD, em conjunto com a própria LGPD, concentra grande parte de suas disposições em salvaguardas contratuais, solicitações do titular e outras formalidades que, embora relevantes, não parecem cobrir de forma satisfatória a dimensão substancial do direito à privacidade, descrita por Schreiber (2014), Bart van der Sloot (2017b) e Hert e Gutwirth (2009). Segundo Lukács (2016) e Doneda (2006), a privacidade tem raízes históricas e contextos sociais que extrapolam meras regras de conduta, pois resulta do incômodo gerado pela vida em aglomerações urbanas e pela exposição ininterrupta do indivíduo ao domínio coletivo. Nesse sentido, pode-se dizer que as normas em vigor carecem de uma abordagem que vá além do cumprimento de cláusulas ou da adoção de padrões contratuais mínimos, refletindo pouco sobre as tensões políticas e culturais próprias do tratamento de dados em escala global.

Segundo Sloot (2017b), o cerne da proteção de dados atualmente envolve tanto sujeitos concretos quanto grupos inteiros, cujos dados são tratados de forma indiscriminada e, por vezes, sem consentimento direto de cada integrante, de modo que o autor demonstra a preocupação para que as demandas de privacidade sejam analisadas, também, *in abstrato*. As exigências colocadas pela resolução chegam a parecer inócuas quando as corporações dispõem de poder econômico e tecnológico

para contornar ou diluir as obrigações formais, deixando a proteção de grupos vulneráveis relegada a um plano secundário.

À título de exemplo, conforme Rouvroy e Poullet (2009), esse vácuo poderia ser mitigado pela previsão de ações coletivas ou instrumentos que reconheçam as violações massivas de dados como uma ofensa a toda a comunidade, e não apenas a indivíduos isolados, o que Sloot (2017b) descreve como sendo a *actio popularis* do Direito à Privacidade. Contudo, a LGPD e a Resolução nº 19/2024 mantêm uma lógica centrada em litígios individuais, o que dificulta a proteção efetiva contra algoritmos que discriminam e catalogam pessoas em escala global.

Nesse sentido, há uma ausência notável de reflexão sobre o caráter coletivo da privacidade quando se fala em transferência internacional de dados. Segundo Doneda (2006), a privacidade deixa de ser meramente subjetiva e adquire contornos de bem jurídico coletivo, pois qualquer vazamento ou tratamento abusivo repercute em toda a coletividade, não apenas em um titular específico. No contexto da transferência internacional de dados, a ameaça se dá pela dimensão infinitésimal dos dados nos fluxos transfronteiriços de dados pessoais. Nesse aspecto, a LGPD e a Resolução nº 19/2024 parecem incidir primordialmente em hipóteses de consentimento ou na avaliação do nível de proteção de país estrangeiro, sem contemplar devidamente a ideia de que a sociedade também possui um direito difuso a não ser exposta a fluxos incontroláveis de dados.

A restrição da análise de danos a situações em que há clara identificação e individualização do titular leva a uma proteção apenas formal, reforçada pela linguagem contratual da Resolução nº 19/2024. Segundo Sloot (2017b), esse caminho gera dificuldade na tutela de situações em que, por exemplo, algoritmos reúnem dados de milhares de pessoas para categorizações estatísticas – expondo a dificuldade da proteção de dados *ratione materiae* –, sem que seja possível atribuir diretamente a cada indivíduo uma ofensa imediata – dada a deficiência do princípio *ratione personae*. A legislação, nesse aspecto, pode operar como um instrumento que legitima determinadas práticas de vigilância em massa, na medida em que só reage a violações direcionadas e plenamente identificadas.

Uma crítica adicional recai sobre o conceito de adequação aos princípios de privacidade, especialmente quando se discute a transferência de dados para países com graus de proteção diferentes. Segundo apontado por Moore (2008), Lukács

(2016), Kuner (2010c; 2009b), as diferenças culturais e históricas na concepção de privacidade são essenciais para identificar até que ponto um ordenamento estrangeiro efetivamente assegura a dignidade do sujeito. Entretanto, a Resolução nº 19/2024 e a LGPD enfatizam a comprovação de garantias, sem se aprofundar em como essas garantias dialogam com a moral e a cultura locais, reduzindo a complexidade do debate a um *checklist* burocrático que avalia unicamente a compatibilidade formal dos sistemas jurídicos.

Outro ponto de crítica diz respeito ao consentimento informado. Embora a Resolução nº 19/2024 e a LGPD contemplem direitos de informação ao titular, há um evidente abismo entre a previsão legal e a capacidade real de compreensão dos indivíduos, sobretudo em contextos de coleta de dados em larga escala. Segundo Laura Schertel Mendes e Gabriel C. Soares (2020), a própria ideia de liberdade individual, que subjaz ao direito à privacidade, esbarra na dificuldade de o sujeito comum avaliar riscos tecnológicos com discernimento e tempo suficientes. Quando o texto normativo presume que o consentimento é o ápice da autodeterminação, ignora que grande parte das violações atuais ocorre de forma opaca, valendo-se da baixa percepção do usuário sobre o alcance da vigilância digital.

O descompasso entre a concepção teórica de privacidade, que deveria integrar dignidade, autonomia e não-discriminação, e o enfoque predominantemente contratual e procedimental, leva a um enfraquecimento da proteção jurídica. Isso se dá, também, porque é difícil comparar sistemas de direitos fundamentais (KUNER, 2019). Ademais, os direitos fundamentais, como é o caso do Direito à Privacidade, não podem se reduzir ao contrato (KUNER, 2019). Segundo Schreiber (2014), existe uma dimensão substancial da privacidade que se relaciona ao próprio conteúdo do uso do dado, e não apenas à maneira como ele é coletado ou compartilhado. Contudo, o que se observa na Resolução nº 19/2024 é a perpetuação de uma lógica que, em vez de trazer instrumentos concretos para evitar finalidades abusivas, sustenta-se quase unicamente em formalidades prévias, como as cláusulas-padrão e a validação oficial de termos. Na União Europeia, Kuner (2019) descreve que o excesso de formalidade na Transferência Internacional de Dados não demonstra uma atividade concreta de proteção, alcunhando o termo “Ficção Legal” para a deficiência prática do padrão europeu. Segundo Kuner (2019), o padrão europeu é mais ilusório do que real.

No caso da Europa, é possível concluir que lá, a proteção de dados pessoais perdeu, materialmente, seu *status* de Direito Fundamental para Transferência Internacional de Dados. Isso ocorre porque, quando tal Direito é analisado, tem-se priorizado os interesses econômicos ao invés de se priorizar o Direito Fundamental do Titular com seu valor essencialmente irrenunciável (KUNER, 2019; OLIVEIRA, 2024; SLOOT, 2017b).

Ademais, o art. 4º, incisos I e II, da Resolução n.º 2/2022 da ANPD, que regulamenta o tratamento de dados por agentes de pequeno porte, estabelece os critérios para a classificação do tratamento de dados pessoais como de alto risco, o que exige um nível maior de cuidado e proteção. Para que um tratamento de dados se enquadre nessa categoria, é necessário que dois critérios sejam atendidos simultaneamente: um critério geral e um critério específico.

Os critérios gerais determinam situações em que o volume ou o impacto do tratamento de dados pode gerar riscos mais amplos (inciso I). Um desses critérios ocorre quando há tratamento de dados em larga escala, ou seja, quando uma grande quantidade de informações pessoais é coletada e processada, aumentando o potencial de exposição e vulnerabilidade dos titulares (alínea “a”, inciso I). Outro critério se dá quando o tratamento de dados afeta significativamente os interesses e direitos fundamentais dos indivíduos, o que pode comprometer a privacidade, a segurança ou outros direitos essenciais (alínea “b”, inciso I).

Já os critérios específicos dizem respeito à forma como os dados estão sendo tratados (inciso II). Um deles envolve o uso de tecnologias emergentes ou inovadoras, que podem apresentar riscos desconhecidos, como inteligência artificial, reconhecimento facial e outras soluções avançadas (alínea a). A alínea “b” estabelece a vigilância ou controle de espaços acessíveis ao público, como câmeras de segurança em locais movimentados que monitoram o comportamento das pessoas. Além disso, o tratamento de dados pode ser considerado de alto risco quando envolve decisões tomadas exclusivamente por algoritmos, ou seja, quando um sistema automatizado define aspectos do perfil pessoal, profissional, de saúde, de consumo ou de crédito de alguém sem qualquer intervenção humana (alínea “c”). Por fim, há um risco elevado no uso de dados sensíveis ou de informações pessoais de grupos vulneráveis, como crianças, adolescentes e idosos, que requerem proteção legal reforçada (alínea “d”).

O Regulamento de Transferência Internacional de Dados (Resolução n. 19/2024, da ANPD) não estabelece essa previsão, enquanto o regulamento voltado para agentes de pequeno porte (Resolução n. 02/2022, da ANPD) o faz. A diferença evidencia uma contradição na atuação da ANPD, que impõe requisitos mais rigorosos para operações de menor impacto e, ao mesmo tempo, deixa de prever salvaguardas similares para transferências internacionais, que apresentam riscos significativamente maiores.

A regulamentação para agentes de pequeno porte parte da premissa de que essas entidades possuem menor capacidade operacional e financeira para cumprir todas as exigências da Lei Geral de Proteção de Dados (LGPD), o que justifica a adaptação de certas obrigações. No entanto, ao garantir esse cuidado, a ANPD reconhece que diferentes contextos de tratamento de dados demandam regras proporcionais ao seu nível de risco.

O problema surge quando essa lógica não é aplicada à transferência internacional de dados, que envolve fluxos transfronteiriços de informações, diferentes jurisdições e potenciais lacunas regulatórias, tornando-se um dos pontos mais críticos da proteção de dados pessoais. Enquanto pequenas empresas e startups nacionais recebem um tratamento normativo detalhado, a circulação de dados para países terceiros, que pode envolver grandes corporações, ausência de garantias adequadas e impactos na soberania, permanece sem a devida previsão normativa.

A mencionada disparidade na regulamentação enfraquece a coerência da atuação da ANPD e pode comprometer a segurança jurídica, pois sugere que a Autoridade optou por detalhar regras para situações de menor impacto, ao passo que negligenciou um tema que afeta diretamente a proteção dos direitos fundamentais dos titulares de dados em escala global.

A proteção de dados pessoais no Brasil, reconhecida pela Emenda Constitucional nº 115/2022 como direito fundamental de eficácia limitada, gera tensão quando posta em confronto com a dimensão mais ampla da privacidade, já consagrada no art. 5º, X, da Constituição, como direito fundamental de eficácia plena. A partir das constatações de Rouvroy e Poullet (2009), o risco desse deslocamento normativo se manifesta quando o consentimento do titular passa a

legitimar operações mercantis de dados, esvaziando o cerne da autodeterminação informativa.

Há uma contradição evidente no fato de a Constituição Federal de 1988 tutelar a privacidade como direito fundamental e, ao mesmo tempo, condicionar a efetivação do direito à proteção de dados a regulamentações infraconstitucionais. A partir das contribuições de Hert e Gutwirth (2009), essa lógica formal pode resultar em uma leitura parcial, que ignora o potencial transformador – da concepção constitucional de Lessig (1996) – de se reconhecer a proteção de dados como um direito constitucional de aplicação imediata.

A Emenda Constitucional nº 115/2022 cristaliza essa tensão ao estabelecer a proteção de dados como um direito dependente de lei específica, relegando, na prática, a concretização material do direito a instrumentos legais que podem priorizar interesses de mercado (KUNER, 2010c; KUNER et al., 2013a; KUNER et al., 2019), violando a concretização de um constitucionalismo material de proteção de dados, conforme apontado por Hert e Gutwirth (2009). A apropriação dos dados não se reduz a um contrato livremente negociado, mas acarreta a mercantilização do próprio sujeito (KUNER, 2010c; KUNER et al., 2013a; KUNER et al., 2019), o que afronta a dignidade humana tutelada pelo art. 1º, III, da Constituição (FRANCO, 2009). A Resolução nº 19/2024 da ANPD, por exemplo, foca em aspectos contratuais e procedimentais para viabilizar transferências internacionais de dados, mas não enfrenta a fundo a repersonalização do sujeito, isto é, a garantia de que a coleta e o tratamento de informações não inviabilizem o desenvolvimento de sua personalidade e não afetem a privacidade.

O esvaziamento do caráter imediato do Direito à Privacidade tende a enfraquecer a resposta jurídica frente às rápidas transformações tecnológicas, mantendo o aparato legal em um nível procedimental que pouco assegura a autodeterminação informativa e a desmercantilização da vida, valores centrais que, de acordo com a leitura integrativa de Dworkin (1985; 1986), deveriam ser o verdadeiro fundamento de qualquer lei ou regulamento sobre o tema.

De acordo com Suda (2017), a ideia original do *Datenschutz* alemão é justamente sustentar um equilíbrio político entre a privacidade e o uso controlado das informações, preservando a dignidade do titular. A decisão do *Bundesverfassungsgericht* (1983) enfatizava que a autodeterminação informativa

exige capacidade real de intervenção do titular (ROUVROY; POULLET, 2009). Contudo, a adoção de mecanismos excessivamente individualistas, presentes tanto na LGPD quanto na Resolução nº 19/2024, transforma a proteção de dados em um exercício meramente procedimental, de modo que o sujeito fica impossibilitado de conferir que o processo de tratamento corresponde às expectativas do consentimento (ROUVROY; POULLET, 2009).

Se a implementação dos padrões europeus de proteção de dados, segundo perspectiva de Mantovani (2020), representam a contratualização da sociedade, em uma perspectiva de Direitos Fundamentais, ao invés de se observar um movimento de constitucionalização do direito com a perspectiva da transferência internacional de dados, vê-se a contratualização do Direito Constitucional, porque a proteção de um direito fundamental é delegada, essencialmente, à convenção das partes. A introdução do Direito à Proteção de Dados no rol de Direitos Fundamentais faz com, um direito que era considerado de eficácia plena, conforme art. 5, X, da CRFB/88, passe a ser interpretado como um Direito de Eficácia Limitada.

Segundo Sloot (2017b), o critério de autonomia jurídica do direito à proteção de dados implicaria que a proteção de dados pudesse operar sem se vincular a valores mais amplos, como a privacidade ou o livre desenvolvimento da personalidade. Contudo, o próprio arcabouço da LGPD e da Resolução nº 19/2024 mostra que os dispositivos de consentimento, transparência e a regulação contratual das transferências internacionais de dados são, em essência, mecanismos de tutela do sujeito contra a exposição arbitrária de sua esfera íntima, o que revela a dependência do direito à proteção de dados em relação ao direito à privacidade. Quando a legislação brasileira se concentra em estipular deveres contratuais para a transferência internacional de dados ignora a advertência de que o núcleo ético do direito à proteção de dados só tem sentido se medido contra o parâmetro mais amplo do direito à privacidade. Isso aparece claramente na Resolução nº 19/2024, que dispõe sobre cláusulas-padrão contratuais e outras formalidades, mas não oferece uma salvaguarda eficaz para situações em que a proteção de dados, mesmo observando a “legalidade”, possa ainda violar a privacidade por arbitrariedade (RENGEL, 2013).

Esse vácuo procede da insistência em tratar a proteção de dados como algo independente, esquecendo que o grau de efetividade desse direito é determinado

por sua capacidade de resguardar a privacidade contra intromissões, o que mostra, por consequência, que não se trata de um direito inteiramente autônomo.

A própria Emenda Constitucional nº 115/2022, ao colocar o direito à proteção de dados em patamar constitucional, parece caminhar na contramão das críticas de Sloot (2017b). Se a ideia fosse manter o sujeito no centro da proteção, a legislação precisaria explicitar em que medida essa "fundamentalização" não colide com o fato de que, nas relações concretas, muitas vezes o que se protege é o fluxo econômico de dados, e não o titular de forma plena, de acordo com a crítica de Sloot (2017b).

A Resolução nº 19/2024 exemplifica bem essa contradição: ao detalhar mecanismos de transferência internacional, assegura apenas que tais fluxos cumpram requisitos legais, mas não enfrenta como, no plano material, tais transações podem redundar em vigilância sistemática e genralizada. Em resumo, a suposta autonomia do direito à proteção de dados termina por ocultar a realidade de que é na privacidade, em sentido substantivo, que reside o juízo de proporcionalidade ou desproporcionalidade do tratamento de dados.

A evidenciada limitação normativa reflete, a partir das considerações de Tzanou (2013), o que se pode chamar de "ilusão da liberdade afirmativa", ou seja, a crença de que conceder autonomia formal ao sujeito no gerenciamento de seus dados resolveria, por si só, as violações de privacidade. E, assim, a liberdade negativa não importa, por ser um "outro" direito.

Em resumo, a tentativa de criar um regime autônomo e autosuficiente para a proteção de dados termina por esvaziar o papel da privacidade como parâmetro fundamental, sobretudo nos casos em que o tratamento de dados segue todas as exigências legais, mas ainda assim viola a dignidade do titular ou de grupos inteiros (SLOOT, 2017B; RENGEL, 2013).

A forma como a LGPD e a Resolução nº 19/2024 da ANPD estruturam a transferência internacional de dados pessoais não reflete a compreensão do direito à privacidade como uma norma de *jus cogens*, pois privilegiam requisitos contratuais e níveis de proteção considerados "adequados" sem contemplar, de maneira robusta, a inalienabilidade do direito à privacidade. Segundo Linderfalk (2013), normas de *jus cogens* seriam inderrogáveis mesmo por tratados, pois cumprem uma função central de salvaguarda dos direitos humanos, o que, no contexto brasileiro, exigiria um regime mais rígido e inequivocamente protetivo para as transferências de dados,

sem espaço para relativizações que subordinem a privacidade a interesses econômicos.

Atribuir status de *jus cogens* à privacidade implicaria reconhecer sua supremacia frente a legislações nacionais ou conveniências mercantis (KURAT, 2023a; KURAT, 2023b; KRAMER, 2024), o que é pouco refletido no texto legal brasileiro, centrado em mecanismos de adequação e consentimento. Ao não tratar a privacidade como pilar inegociável, a legislação pode legitimar a circulação de dados em cenários onde os sujeitos não dispõem de meios concretos para impedir a instrumentalização de suas informações pessoais.

A Resolução nº 19/2024, ao detalhar hipóteses como cláusulas contratuais específicas ou mecanismos de homologação internacional, segue uma abordagem que se alinha mais a interesses comerciais do que à concepção de privacidade como direito humano fundamental e universal. Kramer (2024) enfatiza que, em meio à expansão digital, a privacidade deve receber prioridade absoluta, por ser a garantia de uma vida digna livre de vigilância desmedida. Contudo, o quadro normativo nacional não chega a reconhecer essa prevalência incondicional do direito à privacidade, uma vez que a ênfase recai sobre o cumprimento de obrigações formais, não sobre a vedação intransigente de fluxos que descumpram padrões humanitários mínimos.

Ainda que a LGPD procure delimitar hipóteses legais de tratamento, faltam disposições que acolham, de modo inequívoco, concepções sobre a intangibilidade da privacidade, como a abordagem feita por Kramer (2024) e Kurat (2023a; 2023b). Na prática, o consentimento, figura central do regime, não resolve as situações em que grupos em vulnerabilidade se tornam alvo de violação sistemática, conforme apontam Kuner et al. (2017), Couldry e Magalhães (2021) e Silva e Nascimento (2023), ao analisar o uso de Tecnologias de Informação e Comunicação na ajuda humanitária em zonas de conflito.

Caso se adotasse a perspectiva de *jus cogens*, a transferência internacional de dados para países sem garantias sólidas de proteção seria inviável por definição, em vez de mera hipótese a ser condicionada a contratos. Como ressalta Kramer (2024), o direito à privacidade deveria ser intransponível, exigindo que qualquer acordo comercial ou cooperação governamental respeitasse prioritariamente a autonomia e a segurança dos titulares.

Em conclusão, a leitura da LGPD e da Resolução nº 19/2024 à luz da concepção de que o direito à privacidade seria *jus cogens* expõe uma dissonância fundamental. Ao invés de promover uma defesa irrestrita da esfera íntima e dignidade humana, o ordenamento brasileiro mantém-se atrelado a uma lógica de adequação procedimental, consentimentos formais e avaliação superficial de risco, silenciando sobre a força imperativa e universal da privacidade na seara internacional. Assim, as normas internas brasileiras, tal como estão, carecem de mecanismos efetivos para resguardar a privacidade como direito inviolável, passando ao largo do reconhecimento de seu status de norma cogente e, portanto, não negociável.

A forma como a LGPD e a Resolução nº 19/2024 da ANPD disciplinam a transferência internacional de dados pessoais revela, em grande medida, um paradigma que não leva em conta a complexidade jusfundamental que o fenômeno atual dos fluxos de dados exige. Embora a legislação nacional busque prever mecanismos de adequação e supostas garantias contratuais, não há, de fato, uma preocupação clara em lidar com as incertezas jurisdicionais que emergem quando o ambiente digital elimina as fronteiras entre Estados (ANDREWS, 2020).

Ao aplicar rigidamente disposições contratuais e exigências formais sem enfrentar o problema do “onde” e do “quem” julga ou regula, as normas brasileiras deixam em aberto um vácuo sobre a efetividade de suas próprias disposições em cenários extraterritoriais.

Nesse ponto, a crítica de Svantesson (2017) sobre o declínio do princípio da territorialidade se faz especialmente pertinente: a legislação foca em regular o “para onde” os dados vão, mas não avança no “como” — ou seja, não enfrenta as distintas e, por vezes, sobrepostas jurisdições que incidem no ciberespaço, gerando insegurança jurídica para titulares e agentes de tratamento.

Embora a União Europeia tenha desenvolvido um regime mais expansivo e baseado na ideia de “a lei acompanha o dado”, conforme observa Kuner (2021), o modelo brasileiro ainda parece incipiente em conciliar tal fundamento com as exigências locais de proteção, principalmente porque as obrigações da ANPD não definem com clareza de que modo ocorre a fiscalização efetiva em território estrangeiro. Ou seja, seguindo a análise de Svantesson (2017), fixar contratos ou exigir consentimentos formais não equaciona o desafio de quem pode, de fato,

exercer jurisdição prescritiva ou adjudicativa quando o litígio se desenrola fora das fronteiras brasileiras.

Essa falta de clareza quanto aos critérios de conexão substancial, interesse legítimo e razoabilidade — princípios que, segundo Svantesson (2017), deveriam reger as reivindicações de jurisdição — faz com que a legislação se restrinja à tentativa de impor salvaguardas contratuais e decisão de adequação, confiando excessivamente em acordos privados e decisões estatais para assegurar garantias públicas de privacidade.

Contudo, em um cenário em que empresas multinacionais manejam dados dispersos em inúmeras localizações, as exigências contratuais e as decisões estatais se mostram insuficientes para robustecer a capacidade real de fiscalização brasileira. Como destaca Kuner (2009a), sem harmonização jurídica efetiva ou instrumentos multilaterais de cooperação, o princípio da personalidade e a extraterritorialidade das disposições locais acabam esbarrando em entraves práticos, sobretudo quando não há consenso internacional sobre os padrões de proteção de dados.

Ao privilegiar uma visão que aposta em autorizações pontuais e requisitos de adequação, a legislação nacional não estabelece mecanismos concretos para lidar com países classificados como “paraísos de dados” — jurisdições cujas leis seriam muito menos protetivas e que, na prática, atraem operações de tratamento, dificultando a supervisão (ANGARITA; ZULUAGA, 2019; SUDA, 2017; OLDANI, 2020). Conforme Kuner (2010c) adverte, a mera previsão de exigências de adequação não resolve as barreiras de *enforcement*, sobretudo se não houver cooperação internacional eficaz ou alguma convergência normativa que vá além de listas e pareceres unilaterais.

Outro ponto grave, é a distinção entre transferência internacional de dados e Coleta internacional de dados, feita pela LGPD e pelo Regulamento Internacional de Dados Pessoais do Brasil. De acordo com Santos (2023, p. 123), “a transferência internacional implica necessariamente no envio de dados entre dois ou mais agentes localizados em países distintos, enquanto a coleta internacional de dados é realizada diretamente por um único agente situado no exterior”.

A distinção estabelecida pela legislação, conforme explicada por Santos (2023), faz sentido sob uma perspectiva analítica. No entanto, é evidente que tal

característica ignora pontos-chave e, consequentemente, impõe limitações práticas significativas. A principal delas é que a LGPD, o GDPR e o Direito Internacional Público, de modo geral, aplicam-se com base na jurisdição, e não na quantidade de agentes envolvidos. Svantesson (2016) afirma que o debate contemporâneo sobre privacidade não escapa da questão jurisdicional.

Assim, não se avalia, para fins de definição da proteção jurisdicional, se a empresa estrangeira está coletando ou recebendo dados de outro agente, mas sim se sua atividade interfere em dados de titulares localizados em outra jurisdição. Isso porque, a jurisdição não é uma questão matemática, de modo que sua aplicação não pode ser reduzida a cálculos. Dessa forma, a distinção entre coleta e transferência compromete a definição de um critério seguro para o exercício da jurisdição.

O segundo aspecto é o persistente distanciamento ontológico da LGPD e, igualmente, do GDPR, pois o fluxo de dados não é algo estanque, de modo que não pode ser definido por categorias simplificadas que se concentram em aspectos isolados, como “transferência” e “coleta”. Por exemplo, serviços digitais operados no exterior podem coletar dados diretamente de usuários de outro país, mas o processamento pode envolver terceiros em diversas jurisdições, configurando fluxos mais complexos. Ou seja, essa distinção é extremamente artificial. No ciberespaço, devido à ausência de fronteiras físicas na circulação de dados, é difícil delimitar rigidamente o que constitui coleta e o que configura transferência, especialmente quando os marcos regulatórios citados adotam abordagens simplificadas e superficiais. O fenômeno, no entanto, é extremamente complexo e exige um tratamento mais adequado. A distintação entre coleta internacional de dados e transferência internacional de dados servirá para dissolver gradualmente a proteção dos titulares de dados.

Bart van der Sloot (2017b) argumenta que é necessária uma perspectiva de “privacidade de grupo”, conforme destacado na seção 2.1, tendo em vista a constante dificuldade de pessoalizar as transferências de dados, bem como as transferências internacionais de dados pessoais. Kuner et. al (2012) descrevem que é preciso que os reguladores compreendam o desafio imposto pelo *Big Data*, e tomem consciência da exponencialidade dos fluxos transfronteiriços de dados, conferindo atenção peculiar para este caso. Ou seja, é preciso regular, em algum sentido, os dados que são transferidos em massa (KUNER et. al., 2012).

Além disso, a noção de transferência internacional de dados, quando ampliada para incluir tanto as transferências deliberadas quanto o acesso permitido a dados pessoais, traz uma perspectiva mais abrangente e realista para a proteção de informações no ambiente digital (ESPEEL; COLSON; CRUQUENAIRE, 2022). Ou seja, os dados podem cruzar fronteiras de formas nem sempre intencionais, como no caso de redirecionamentos automáticos por configurações de rede, sem que o controlador ou processador tenha pleno conhecimento ou intenção de que isso ocorra (ESPEEL; COLSON; CRUQUENAIRE, 2022). No entanto, basear a definição de transferência apenas no conhecimento ou intenção do controlador pode criar lacunas na proteção, já que situações não intencionais poderiam escapar ao controle regulatório, deixando os titulares desprotegidos (ESPEEL; COLSON; CRUQUENAIRE, 2022).

Em síntese, a transferência internacional de dados, tal como regulada pela LGPD e operacionalizada pela Resolução nº 19/2024, encontra obstáculos evidentes ao se confrontar com os dilemas jurisdicionais detalhados por Kuner (2010c) e Svantesson (2017). O ordenamento brasileiro se mantém demasiadamente apegado aos modelos contratuais e à ficção de que o consentimento ou as autorizações estatais resolvem por si sós as complexidades do ciberespaço.

Ao deixar em segundo plano uma reflexão aprofundada sobre como efetivar a jurisdição prescritiva, adjudicativa e, sobretudo, executiva em âmbito transnacional, a legislação corre o risco de perpetuar incertezas, aumentar custos de transação para empresas e, mais grave, fragilizar a real proteção de direitos dos titulares. Se, por um lado, a ênfase em salvaguardas contratuais e consentimento pode trazer maior previsibilidade formal, por outro, ignora a advertência de Kuner (2009a) de que, sem uma abordagem cooperativa e global, o princípio da personalidade se choca inevitavelmente com culturas jurídicas territoriais, resultando em conflitos e inseguranças que as regras internas, isoladamente, não conseguem resolver.

A Resolução nº 19/2024 da ANPD, em conjunto com a LGPD, propõe um regime de transferência internacional de dados pessoais que, à primeira vista, lembra a construção europeia pautada pelo GDPR e pela Convenção 108+. Contudo, ao se analisar o detalhamento europeu sobre cláusulas-padrão contratuais, decisões de adequação e estatutos de bloqueio, torna-se evidente que o ordenamento brasileiro, embora formalmente complexo, não alcança a mesma

profundidade na proteção de dados quando os fluxos extrapolam as fronteiras nacionais. Segundo Terwangne (2022), a Europa estabelece um arcabouço amplamente testado no Tribunal de Justiça da União Europeia, sobretudo em decisões como Schrems I e Schrems II.

Ainda que a Resolução nº 19/2024 tenha buscado criar mecanismos de validação prévia e verificação de cláusulas contratuais específicas, carece de um dispositivo que se assemelhe à prerrogativa europeia de bloquear decisões extraterritoriais que demandem a entrega de dados pessoais, independentemente da vontade do controlador, presente no art. 48 do GDPR. Segundo Kuner (2020e), essa proteção “de bloqueio” reforça a soberania regulatória europeia e assegura que mesmo uma ordem judicial estrangeira não se sobreponha automaticamente aos padrões do GDPR.

No Brasil, a ausência de um regime análogo deixa as decisões judiciais e administrativas de outros países em terreno indefinido, sem uma salvaguarda legal clara para impedir a transferência compulsória de dados. O Direito à Privacidade e à Proteção de Dados, embora formalmente reconhecidos, são constantemente desafiados por lacunas regulatórias que inviabilizam sua aplicação prática. A ausência de um estatuto de bloqueio, como o previsto no artigo 48 do GDPR, reflete uma falha crítica na proteção da soberania regulatória brasileira. Sem esse instrumento, o Brasil se torna vulnerável a intromissões de outras jurisdições, permitindo que legislações estrangeiras determinem, em última análise, o destino dos dados coletados em território nacional.

Seguindo a análise de Bräutigam (2016), o estatuto de bloqueio do art. 48 do GDPR pode ter sido incluído para explicar que o cumprimento de uma obrigação legal, conforme previsto no art. 6, “c”, do GDPR, como elemento caracterizador da licitude do processamento, não pudesse ser invocado para justificar uma transferência internacional de dados quando envolvesse o cumprimento de decisão proferida por um agente de outra jurisdição.

Isso sugere, no contexto brasileiro, a hipótese de que jurisdições estrangeiras poderiam se sobrepor à jurisdição do Brasil com base no art. 7º, II, da LGPD, que entende ser lícito o processamento quando fundado no cumprimento de obrigação legal. No caso do Brasil, tal situação se torna ainda mais preocupante, pois o art. 7º,

II, da LGPD, estatui, também, a “obrigação regulatória do controlador” como uma base legal para o processamento de dados pessoais.

Além dessa sistemática, o estatuto de bloqueio possui uma justificativa política de grande importância, pois, por meio dele, é possível protestar contra intromissões de outras jurisdições (BRÄUTIGAM, 2016) e afirmar a soberania regulatória do país no campo da proteção de dados. Em conclusão, a ausência desse estatuto compromete não apenas a proteção dos titulares de dados, mas também a credibilidade do marco regulatório brasileiro no cenário internacional.

A falta de exigência para que controladores e operadores de dados localizados fora do território nacional designem representantes legais no Brasil cria um vácuo de responsabilização. Essa lacuna não apenas dificulta a fiscalização de práticas abusivas, mas também incentiva a evasão de responsabilidades por parte de agentes estrangeiros. O custo de violar dados pessoais no Brasil, sob esse arranjo, é inferior ao custo de conformidade, o que gera um incentivo perverso para que empresas internacionais operem sem qualquer comprometimento com os direitos dos titulares brasileiros.

Outro ponto que reforça a inadequação do modelo regulatório brasileiro é a ausência de revisões periódicas obrigatórias das autorizações para transferências internacionais de dados. O artigo 45 do GDPR estabelece um intervalo de, no mínimo, quatro anos para reavaliações, garantindo que decisões estejam em conformidade com padrões de proteção atualizados. No Brasil, a inexistência de uma previsão semelhante compromete a continuidade da proteção e dá margem para que agentes de tratamento relaxem seus compromissos após a obtenção inicial da autorização. Essa omissão enfraquece ainda mais a confiança dos titulares de dados na regulação nacional e perpetua a sensação de impunidade.

A resolução nº 19/2024 da ANPD também ilustra a ineficiência de um modelo que privilegia formalidades procedimentais em detrimento de soluções substanciais. A falta de atenção à questão jurisdicional é um dos aspectos mais críticos, pois evidencia o descompromisso em enfrentar os desafios centrais da transferência internacional de dados. Sem um mecanismo que delimite claramente a competência jurídica em casos de violações, os titulares brasileiros permanecem desprotegidos contra intervenções externas e práticas abusivas de agentes transnacionais.

Enquanto o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, no artigo 27, especifica a necessidade de um representante formalmente estabelecido na UE para assegurar supervisão direta (KUNER, 2021), a Lei Geral de Proteção de Dados (LGPD) e a Resolução nº 19/2024 não estipulam a obrigatoriedade de constituir um representante legal para o agente de tratamento no Brasil. Dessa forma, a regulamentação brasileira não apenas deixa de impor essa exigência, como também não apresenta mecanismos detalhados de *enforcement* para tal obrigação. Como resultado, quando uma multinacional coleta dados no Brasil, mas mantém servidores no exterior, o mecanismo de responsabilização se mostra menos definido em comparação com a Europa, que fortaleceu suas regras e facilitou a aplicação transfronteiriça do GDPR, inclusive com a imposição de sanções de alto valor.

Há, ainda, uma diferença importante na forma como a Resolução nº 19/2024 aborda as cláusulas-padrão contratuais. Ao se comparar com a evolução da Diretiva 95/46/CE para o GDPR, nota-se que a Europa aperfeiçoou os modelos contratuais com atualizações constantes, refletindo posicionamentos do Tribunal de Justiça da União Europeia (KUNER, 2020b). Já a Resolução brasileira, ao enfatizar salvaguardas “adequadas ou suficientes”, não detalha como deve ocorrer a revisão periódica dessas cláusulas, tampouco como se conduz a efetiva fiscalização de sua implementação na prática. Segundo Kuner (2020b), o caso Schrems I consolidou na UE a necessidade de verificar continuamente se o país de destino mantém o nível de proteção exigido, algo que a legislação brasileira não regula de forma tão minuciosa. No art. 45 do GDPR, a revisão da decisão de adequação deve ser de, no mínimo, de 04 em 04 anos.

Vale reconhecer que, assim como o GDPR indica hipóteses de derrogação no art. 49, a LGPD e a Resolução nº 19/2024 também admitem exceções para situações como as que envolvem a proteção de vida ou de incolumidade física. Entretanto, a comparação com o padrão europeu revela que tais exceções, no Brasil, assumem um caráter amplo (KRAMCSÁK, 2024), ao passo que, na UE, há uma cultura de aplicá-las em *ultima ratio* para evitar o desvirtuamento das regras de transferência (KRAMCSÁK, 2024; KUNER, 2020f; MARELLI, 2023). Sem uma orientação oficial clara da ANPD e da LGPD que limite o uso indiscriminado dessas exceções (KRAMCSÁK, 2024), corre-se o risco de banalização das hipóteses de

derrogação, inviabilizando na prática a aplicação rigorosa das salvaguardas contratuais.

Observa-se que, embora a LGPD e a Resolução nº 19/2024 se inspirem fortemente nas soluções europeias para a transferência internacional de dados, persistem brechas significativas na proteção efetiva do titular. Faltam mecanismos análogos ao art. 48 do GDPR para bloquear extraterritorialidades abusivas e falta também uma cultura de justiciabilidade que sustente, no dia a dia, as exigências de "equivalência" de proteção ou a revisão periódica do cumprimento das cláusulas. Dessa forma, o Brasil ainda não alcança a posição de "padrão ouro" em matéria de transferência internacional de dados, evidenciando a necessidade de um aperfeiçoamento regulatório que vá além da mera adoção formal de instrumentos contratuais e normas genéricas, aproximando-se de um regime efetivamente robusto.

A Resolução nº 19/2024 da ANPD e a própria LGPD, embora representem avanços na regulação da transferência internacional de dados, revelam uma preocupante falta de compromisso com a construção de mecanismos de interoperabilidade regional na América Latina. A destacada lacuna reforça o quadro de assimetrias descrito por Belli et al. (2024), no qual a região permanece refém de uma dinâmica de dependência tecnológica e jurídica, reproduzindo padrões coloniais que fragilizam a soberania digital dos países latino-americanos.

Enquanto a legislação brasileira busca uma aparência de convergência com padrões globais, como os estabelecidos pelo GDPR europeu, a realidade econômica e política do Brasil e da região mantém a proteção de dados em um patamar de vulnerabilidade, conforme apontado por Silva e Nascimento (2023). A ausência de uma estratégia robusta para fomentar a cooperação regional e a harmonização normativa resulta em uma dependência excessiva de cláusulas contratuais unilaterais e regimes estrangeiros, que pouco consideram as particularidades e necessidades locais. A fragilidade não apenas compromete a eficácia da proteção de dados na região, mas também perpetua uma relação de subordinação tecnológica e jurídica, distanciando a América Latina de uma verdadeira autonomia digital e de uma governança de dados que priorize os interesses de seus cidadãos.

Mesmo a Resolução nº 19/2024, ao estabelecer procedimentos para legitimar transferências internacionais de dados, ignora em grande medida o risco de

perpetuar práticas de “paraísos de dados” quando lida-se com países cujas regulamentações são menos rigorosas ou cujo poder econômico impõe condições unilaterais (ANGARITA; ZULUAGA, 2019; SUDA, 2017). Segundo Belli et al. (2024), a América Latina, por não ter uma regulação regional minimamente coesa, fica sujeita à imposição de modelos externos, seja o europeu, seja o norte-americano, sem construir uma “proteção de dados tropicalizada” que integre as especificidades culturais, econômicas e sociais locais. Isso se agrava quando se observa que o Brasil não possui uma estratégia clara para enfrentar pressões vindas de atores globais hegemônicos, o que frequentemente resulta em uma flexibilização das exigências que deveria proteger efetivamente o titular.

Ao seguir uma lógica próxima à do GDPR, mas sem adotar uma robustez institucional própria, o ordenamento brasileiro acaba reproduzindo a dicotomia entre o discurso formal de proteção e a realidade concreta de vulnerabilidade do usuário. Tais críticas ecoam a constatação de Silva e Nascimento (2023) de que a subsunção aos interesses globais privilegia grandes atores do mercado e neutraliza, na prática, a capacidade de responsabilização diante de violações.

Em vez de promover um modelo adaptado, capaz de responder às necessidades específicas da população latino-americana — marcada por desigualdades e histórico de exploração de dados, sobretudo sobre grupos vulneráveis —, a legislação brasileira aposta em cláusulas e salvaguardas genéricas, sem consolidar um instrumento verdadeiramente regional. Assim, mesmo a Resolução nº 19/2024, ao cuidar das transferências internacionais de dados, não enfrenta a questão do desequilíbrio estrutural entre nações, perpetuando a fragilidade que Belli et al. (2024) descrevem como um dos traços mais críticos da proteção de dados na América Latina.

Em conclusão, embora a Resolução nº 19/2024 e a LGPD representem um progresso significativo no tratamento jurídico das transferências internacionais de dados, elas se mostram excessivamente baseadas em formalidades contratuais e em hipóteses de consentimento que nem sempre refletem o caráter coletivo e substancial da privacidade. Ao reforçar uma visão individualista da autodeterminação informativa, as normas brasileiras acabam negligenciando aspectos mais profundos, como a vigilância sistêmica e a proteção de grupos vulneráveis. De modo semelhante, ao priorizar a comprovação de “adequação” ou de “garantias formais”, a

legislação raramente se aprofunda na dimensão ética, cultural e histórica que molda a própria ideia de privacidade, sobretudo em países onde práticas discriminatórias e assimetrias de poder persistem. Dessa forma, persiste um distanciamento entre o discurso legal e a realidade dos fluxos de dados em escala global, com potenciais lacunas na proteção contra violações massivas, algoritmos discriminatórios e situações em que consentimentos pouco informados legitimam atividades invasivas. Além disso, ao condicionar a proteção de dados à eficácia limitada, a Emenda Constitucional nº 115/2022 reforça a tensão entre a privacidade e o direito à proteção de dados. Sem instrumentos mais robustos para limitar ingerências extraterritoriais, enfrentar a mercantilização descontrolada de informações ou salvaguardar as prerrogativas coletivas de grupos inteiros, a garantia de privacidade nas transferências internacionais permanece fragilizada, indicando a necessidade de uma revisão crítica e de um aperfeiçoamento substancial das normas em vigor.

4.3 PRINCIPAIS RECOMENDAÇÕES

Para resgatar os valores essenciais do *Datenschutz* e enfrentar os problemas decorrentes da perda de seu núcleo original, algumas soluções podem ser implementadas. As citadas medidas visam não apenas restaurar a centralidade da autodeterminação informativa e do direito à privacidade, mas também assegurar que a proteção de dados seja efetiva e alinhada aos interesses do titular, em consonância com os princípios que fundamentaram o *Datenschutz*.

Primeiramente, é fundamental que a proteção de dados seja reintegrada à sua essência, colocando a privacidade como núcleo indissociável desse direito. Para isso, o marco regulatório brasileiro deve ser revisto para enfatizar que a proteção de dados não é apenas um direito autônomo, mas uma extensão do direito à privacidade. A legislação pode explicitar essa relação de dependência ao estabelecer que qualquer interpretação de proteção de dados deve ser feita à luz da privacidade e da dignidade da pessoa humana. Isso asseguraria que a proteção de dados não seja tratada como um conjunto de procedimentos estanques, mas como um instrumento para garantir valores fundamentais.

Outra medida essencial é reavaliar o papel do consentimento informado no tratamento de dados. Atualmente, o consentimento tornou-se uma formalidade que muitas vezes ignora a capacidade real do titular de compreender e avaliar os riscos

associados ao uso de suas informações. É necessário criar mecanismos que assegurem que o consentimento seja verdadeiramente livre, informado e específico. Além disso, deveria ser promovida uma política ativa de educação digital, capacitando os indivíduos a exercerem seus direitos de maneira consciente e informada.

No contexto do ciclo de vida dos dados, é crucial que o tratamento seja estritamente vinculado aos interesses originais do titular, conforme previa o *Datenschutz*. Para isso, seria necessário implementar auditorias obrigatórias em todas as etapas do tratamento, assegurando que os dados não sejam utilizados para finalidades incompatíveis com as inicialmente previstas. Além disso, a legislação pode exigir que as empresas e instituições demonstrem, de forma proativa, como os interesses do titular estão sendo preservados durante o uso de seus dados.

A regulação também deve abordar a questão da mercantilização excessiva dos dados pessoais. Isso pode ser feito limitando juridicamente a prática de negociar dados como ativos econômicos, impondo sanções mais severas para empresas que tratem dados de forma desvirtuada, trazendo de volta a centralidade da dignidade humana e da autodeterminação informativa, afastando a proteção de dados da lógica puramente comercial.

É imperativo que o Brasil adote uma abordagem normativa que vá além da mera adequação a padrões internacionais. O país deve liderar pelo exemplo, construindo um marco regulatório que recupere os valores do *Datenschutz* e os adapte ao contexto digital contemporâneo.

O fluxo internacional de dados, como fenômeno característico da era do Big Data, exige uma abordagem regulatória inovadora e adaptada às realidades do ambiente digital globalizado. A regulação atual no Brasil, ao tratar a transferência internacional de dados como um evento estático e isolado, falha em reconhecer a dinâmica anárquica que permeia o ambiente digital. O Big Data, pela sua natureza expansiva e descentralizada, permite a coleta e o processamento massivo de informações, muitas vezes de forma invisível e descontrolada, transcendendo fronteiras jurídicas e ignorando as barreiras normativas. Tal cenário torna obsoleta a concepção tradicional de proteção de dados, que se baseia na identificação específica de danos e na individualização de interesses.

A privacidade, nesse contexto, precisa ser compreendida não apenas como um direito individual, mas como um direito difuso, com dimensões que ultrapassam a proteção de interesses pessoais e se estendem à manutenção de um ambiente digital ético e seguro. A coletivização das violações no contexto do Big Data, em que práticas de vigilância e uso indevido de dados são sistemáticas, dificulta a identificação de um dano personalíssimo e exige uma mudança na forma de conceber a proteção de direitos. A abordagem jurídica tradicional, que privilegia a reparação individual, mostra-se ineficaz diante da abstração e da impessoalidade que caracterizam as violações em larga escala.

Nesse cenário, é essencial que a Autoridade Nacional de Proteção de Dados (ANPD) adote medidas que enfrentem essas especificidades e promovam a efetividade do Direito à Privacidade no âmbito da transferência internacional de dados. Uma dessas medidas seria o reconhecimento expresso da possibilidade de apresentação de petições *in abstrato* por parte dos titulares, ou mesmo de entidades representativas, considerando a probabilidade de dano e a natureza sistêmica das violações. Além de permitir a atuação preventiva, reconhece a vulnerabilidade do titular diante de um sistema de tratamento de dados que, por vezes, opera fora do alcance de sua compreensão ou controle.

É fundamental que a ANPD assuma um papel ativo e proativo no monitoramento das transferências internacionais de dados, promovendo auditorias regulares e revisões periódicas das autorizações concedidas. A ausência de mecanismos de revisão compromete a capacidade de adaptação da regulação às mudanças no cenário global e reforça a percepção de fragilidade do sistema regulatório. Nesse sentido, seria imprescindível a criação de normas que determinem a revisão das autorizações em intervalos regulares, alinhando-se ao padrão europeu previsto no artigo 45 do GDPR. A implementação dessa prática garantiria que as condições iniciais para a autorização continuassem a ser atendidas e que os interesses dos titulares permanecessem protegidos ao longo do tempo.

As mencionadas medidas não apenas enfrentariam os problemas impostos pelo Big Data e pela economia de vigilância, mas também fortaleceriam a soberania regulatória brasileira e a proteção dos titulares em um cenário global marcado pela complexidade e pelo descontrole informacional (BELLI; DONEDA, 2021). Ao adotar uma postura mais firme e inovadora, o Brasil poderia se posicionar como uma

referência internacional em proteção de dados, restaurando a efetividade do Direito à Privacidade no contexto contemporâneo.

Para evitar a perpetuação desse “labirinto kafkiano” e romper com a metáfora do trabalho infrutífero de Sísifo, o Brasil precisa adotar medidas profundas e corajosas. Assim, é imprescindível estabelecer um estatuto de bloqueio robusto, que proteja a soberania regulatória nacional. Também é necessário instituir a obrigatoriedade de representantes legais no Brasil para agentes estrangeiros, criando um ponto de contato direto para responsabilização e fiscalização. Paralelamente, a ANPD deve assumir uma postura mais proativa, implementando revisões periódicas obrigatórias e fortalecendo seus mecanismos de auditoria e supervisão.

A construção de uma regulação que transcenda a mera formalidade e alcance a efetividade requer, ainda, um compromisso renovado com a transparência e a humanização dos processos. Os titulares precisam ter acesso a informações claras e acessíveis sobre seus direitos e as práticas de tratamento de dados. Além disso, é essencial fomentar a cooperação internacional, harmonizando padrões regulatórios e consolidando parcerias que fortaleçam a proteção global da privacidade.

Sem esses ajustes estruturais, a regulação brasileira permanecerá condenada ao fracasso, perpetuando um sistema em que normas e procedimentos são abundantes, mas a proteção real dos direitos é escassa. A coragem para inovar e enfrentar os desafios contemporâneos com soluções efetivas é o único caminho para evitar que o trabalho de proteger dados pessoais se torne, como no mito de Sísifo, um esforço eterno e sem resultados concretos.

A inobservância da relevância internacional do Direito à Privacidade reflete um paradoxo: enquanto esse direito é amplamente reconhecido como essencial para a proteção da dignidade humana e da autonomia individual, sua implementação prática enfrenta graves lacunas, especialmente no contexto das transferências internacionais de dados. No Brasil, a fragilidade do arcabouço regulatório e a ausência de uma política robusta de defesa da privacidade destacam como o país priorizou interesses econômicos e de mercado em detrimento da efetividade desse direito fundamental.

A falta de obrigatoriedade para a realização de estudos de impacto à privacidade nas transferências internacionais de dados é uma das falhas mais

evidentes. Tais estudos são ferramentas indispensáveis para identificar, avaliar e mitigar riscos à privacidade antes que os dados sejam compartilhados além das fronteiras nacionais. Ao desconsiderar essa exigência, o Brasil adota uma postura permissiva que ignora o impacto potencial dessas transferências sobre os titulares. A negligência não apenas compromete a proteção dos dados pessoais, mas também desvaloriza a posição do país no cenário global, onde a realização de avaliações de impacto é considerada uma prática fundamental para a proteção da privacidade.

O problema é exacerbado pela crescente influência do mercado na formulação das políticas de proteção de dados. Ao priorizar os interesses econômicos como nova referência normativa, o Brasil desloca o eixo de proteção do indivíduo para os benefícios empresariais, reduzindo a privacidade a uma *commodity* negociável. Há uma distorção na essência do Direito à Privacidade, que não pode ser tratado como um direito secundário ou subordinado a interesses comerciais. Em vez disso, ele deve ser reconhecido como uma salvaguarda essencial para a liberdade e a dignidade humana, especialmente em um contexto internacional marcado pela exploração massiva de dados pessoais.

A ausência de uma política clara e assertiva para defender a privacidade no âmbito internacional também evidencia um descompromisso com os mandamentos constitucionais. O artigo 5º, inciso X, da Constituição Federal, consagra a inviolabilidade da vida privada como um direito fundamental. No entanto, a regulação brasileira falha em traduzir esse mandamento em medidas concretas que garantam sua efetividade além das fronteiras nacionais. É ainda mais preocupante diante da complexidade das cadeias globais de tratamento de dados, que frequentemente expõem os titulares brasileiros a jurisdições menos protetivas.

Para corrigir essa trajetória, é fundamental que o Brasil adote uma postura proativa na construção de uma política internacional de privacidade. Isso implica, primeiramente, a obrigatoriedade de estudos de impacto à privacidade para todas as transferências internacionais de dados, com foco na identificação de riscos e na mitigação de danos potenciais. Além disso, é crucial que o país promova a harmonização regulatória com padrões internacionais, como o GDPR, fortalecendo a cooperação com outras nações para consolidar uma abordagem global de proteção.

Outra medida indispensável é a reafirmação do Direito à Privacidade como prioridade absoluta na formulação de políticas públicas. Isso exige um esforço para

desvincular a proteção de dados de interesses meramente mercadológicos e colocá-la novamente no centro do debate como um direito fundamental. A criação de uma política nacional de privacidade, que articule ações internas e externas, poderia consolidar o compromisso do Brasil com a proteção desse direito no cenário internacional.

Sem essas mudanças, o Direito à Privacidade continuará a ser tratado como um ideal distante, sem efetividade prática. A relevância internacional desse direito depende, em última análise, da capacidade de cada país de implementar medidas concretas que o protejam, tanto dentro de suas fronteiras quanto no âmbito das relações globais. O Brasil tem a oportunidade de reverter esse quadro, assumindo uma posição de liderança na defesa da privacidade como um valor universal e inegociável.

A ausência de interoperabilidade regional na proteção de dados evidencia uma lacuna crítica na abordagem regulatória brasileira, especialmente considerando o potencial de cooperação e harmonização normativa com outros países latino-americanos. A Lei Geral de Proteção de Dados Pessoais (LGPD) e o Regulamento de Transferência Internacional de Dados demonstram pouca ou nenhuma atenção às especificidades culturais, econômicas e políticas que caracterizam a região. Tal desconexão compromete não apenas a proteção dos dados pessoais, mas também a capacidade do Brasil de se posicionar como líder regional em matéria de privacidade e proteção de dados.

Um dos avanços relevantes observados no direito latino-americano, como a separação entre transmissão e transferência internacional de dados, adotada no México e na Colômbia, representa uma oportunidade perdida para o Brasil. A citada distinção, que atribui diferentes níveis de responsabilidade aos agentes envolvidos, poderia fortalecer o marco regulatório brasileiro ao reconhecer as nuances das operações de tratamento de dados em um contexto global. A incorporação de tais disposições permitiria uma maior precisão normativa e maior proteção aos titulares, sem comprometer a funcionalidade das transferências.

Além disso, a falta de uma perspectiva regional impede que o Brasil explore as vantagens de uma colaboração mais estreita com seus vizinhos. A criação de um conselho ou observatório de Direito à Proteção de Dados na América Latina, por exemplo, poderia servir como um fórum para o desenvolvimento de diretrizes

regionais, troca de boas práticas e promoção de políticas que reflitam as realidades locais (VERONESE, 2023d). Essa iniciativa não apenas fortaleceria a proteção de dados na região, mas também consolidaria o Brasil como um agente ativo na formulação de padrões normativos alinhados às necessidades e especificidades latino-americanas.

O descompasso entre a regulação brasileira e as dinâmicas regionais também compromete a proteção da privacidade em um contexto de crescente integração econômica e tecnológica. A ausência de interoperabilidade cria barreiras para a adoção de padrões conjuntos que poderiam simplificar as transferências de dados entre países, ao mesmo tempo que asseguram níveis adequados de proteção. A inação regulatória perpetua um cenário fragmentado, onde os titulares de dados são os principais prejudicados pela ausência de uma abordagem coordenada.

Propor direções para superar essas deficiências é essencial. Primeiramente, o Brasil deve investir na harmonização regulatória com outros países da América Latina, promovendo acordos bilaterais e multilaterais que estabeleçam padrões mínimos de proteção de dados na região. Isso incluiria a adoção de princípios comuns, como a separação entre transmissão e transferência de dados, e o reconhecimento de mecanismos de supervisão e auditoria que transcendam fronteiras nacionais.

Além disso, é fundamental desenvolver uma agenda de pesquisa que explore as interseções entre regulação de dados e contextos regionais. Estudos que examinem as práticas regulatórias de países vizinhos podem fornecer insights valiosos para a evolução do marco legal brasileiro. A análise de iniciativas bem-sucedidas, como a incorporação de cláusulas específicas para operações transnacionais ou a promoção de certificações regionais de proteção de dados, pode servir como base para futuras reformas legislativas.

Por fim, a promoção da interoperabilidade regional deve ser vista como um passo estratégico para o fortalecimento do Direito à Privacidade no Brasil e na América Latina. A integração normativa não apenas aumentará a eficiência das transferências de dados, mas também consolidará uma narrativa regional que priorize a proteção dos direitos dos titulares. Com uma abordagem mais colaborativa e alinhada às especificidades locais, o Brasil poderá reverter a inefetividade

observada, posicionando-se como um líder regional em privacidade e proteção de dados pessoais.

5 CONSIDERAÇÕES FINAIS

O objetivo I foi cumprido através do item 2, deste documento, ao demonstrar, de forma abrangente, que o direito à privacidade se configura como um alicerce fundamental, transcendendo sua origem histórica ligada exclusivamente à proteção da liberdade individual e à propriedade. A análise realizada enfatizou como o direito à privacidade evoluiu para incorporar dimensões mais amplas, como a autonomia decisória, a autodeterminação informacional, e a participação ativa em sociedade, refletindo uma compreensão mais rica e complexa desse direito em um contexto cada vez mais interconectado e tecnologicamente avançado.

Os itens 3.2, 3.3 e 4.1 cumpriram o objetivo II ao realizarem uma análise comparativa dos diferentes marcos regulatórios nacionais, estrangeiros e internacionais que governam a proteção de dados pessoais e o direito à privacidade. Inicialmente, ele destacou as disposições específicas da legislação da União Europeia, incluindo o Regulamento Geral de Proteção de Dados (GDPR), e suas implicações para as transferências internacionais de dados, ressaltando como essas regras estabelecem padrões rigorosos que devem ser seguidos por outros países. O texto explorou as particularidades dos sistemas jurídicos na América Latina, destacando como países como Argentina, Brasil e México se alinham ou divergem dos padrões europeus. Isso foi exemplificado pelo foco na legislação brasileira, como a Lei Geral de Proteção de Dados (LGPD), e como ela regula a transferência internacional de dados.

O objetivo III, que é diagnosticar as bases legais da transferência internacional de dados pessoais no Brasil, é abordado no texto através de uma exploração detalhada das disposições legais estabelecidas pela Lei Geral de Proteção de Dados Pessoais (LGPD) e pelas regulamentações adicionais emitidas pela Autoridade Nacional de Proteção de Dados (ANPD). Este diagnóstico é realizado ao no item 4.1 deste documento por meio do diagnóstico de artigos específicos da LGPD e da resolução n. 19/2024 da ANPD que regulam as transferências internacionais de dados.

O objetivo IV do texto foi cumprido pelo item 4.2 ao explorar a efetividade do direito à privacidade dos titulares de dados no Brasil, destacando as limitações das abordagens atuais que a legislação brasileira adota, particularmente no contexto da Lei Geral de Proteção de Dados (LGPD) e da Resolução nº 19/2024 da Autoridade Nacional de Proteção de Dados (ANPD). O texto fornece uma análise crítica das disposições legais que se concentram majoritariamente em salvaguardas contratuais e solicitações de consentimento. A abordagem, embora relevante, foi identificada como insuficiente para cobrir a dimensão substancial e coletiva do direito à privacidade.

Neste documento, foi possível validar plenamente a hipótese I. A destacada proposição sugeriu que uma investigação aprofundada dos postulados essenciais do Direito à Proteção de Dados Pessoais traria perspectivas imprescindíveis para a regulação das transferências internacionais de dados, elucidando aspectos vitais para a eficácia do Direito à Privacidade. A fundamentação para essa afirmação derivou de uma análise criteriosa realizada no item 2, que abordou os alicerces do Direito à Privacidade, a constitucionalização do Direito à Proteção de Dados Pessoais, e a avaliação crítica da autonomia jurídica desse direito. Este exame mostrou-se crucial para entender o alcance e a profundidade com que a privacidade é protegida em contextos de transferência de dados além-fronteiras, tema central discutido no item 4.2. Durante essa análise, observou-se, por exemplo, que a dimensão substancial da privacidade passa despercebida na regulação brasileira da transferência internacional de dados pessoais, entre outros fatores relevantes identificados.

Adicionalmente, as hipóteses II e III foram confirmadas neste documento. A hipótese II indicava que entender tanto os aspectos jurisdicionais quanto os padrões regulatórios do GDPR e os da América Latina ajudaria a identificar diferentes níveis de proteção da privacidade. A confirmação emergiu dos diagnósticos consigandos nos subitens 3.1 e 3.2, que abordaram as complexidades jurisdicionais nas transferências internacionais de dados, as exigências do GDPR e os desafios enfrentados pelos sistemas regulatórios latino-americanos.

Integrando essas discussões com as avaliações do subitem 4.1, destinadas a responder à hipótese III — que propunha avaliar a Lei Geral de Proteção de Dados Pessoais (LGPD) do Brasil para compreender se ela oferece um arcabouço

regulatório suficiente para a proteção das transferências internacionais de dados —, consegue esclarecer variados problemas de regulação da transferência internacional de dados, como explorado no subitem 4.2. A pesquisa revelou, por exemplo, que o Brasil, diferentemente da Europa, não possui um estatuto de bloqueio que proíba transferências internacionais de dados, nem exige que agentes de tratamento estrangeiros estabeleçam um representante legal no país. À vista disso, ao negligenciar a soberania regulatória do Brasil em matéria de transferência internacional de dados, o país acaba comprometendo a proteção do direito à privacidade.

Os subitens 4.2 e 4.3 da dissertação confirmaram a hipótese IV, que propunha que a investigação das práticas regulatórias nacionais e internacionais, juntamente com concepções aliadas, auxiliaria na determinação de uma maior efetividade para o direito à privacidade na Transferência Internacional de Dados. O subitem 4.2 investiu em críticas, visando determinar a efetividade do direito à privacidade dentro de um contexto mais amplo abordado na dissertação. Já o subitem 4.3 apresenta uma proposta baseada nas discussões desenvolvidas ao longo do trabalho, consolidando as reflexões e sugerindo caminhos para fortalecer a proteção da privacidade no cenário regulatório brasileiro.

Ao concluir este documento, destaca-se que ele buscou responder à seguinte questão: considerando a regulação da transferência internacional de dados, em que medida o direito à privacidade é efetivamente protegido nos fluxos internacionais de dados pessoais? Tendo alcançado integralmente os objetivos propostos e confirmado as hipóteses delineadas, conforme demonstrado, é possível estabelecer uma série de conclusões que respondem diretamente à problemática inicialmente apresentada. Em conclusão, o Direito à Privacidade é inefetivo na transferência internacional de dados pelas razões seguintes:

I. Adeus à *Datenschutz*: Conforme observado ao longo do trabalho, a proteção de dados emerge a partir da concepção do Direito à Privacidade em um sentido político, cuja finalidade inicial era permitir o uso controlado da exposição de determinadas informações. Foi nesse contexto que surgiu o *Datenschutz* alemão. A narrativa que apresenta o Direito à Proteção de Dados como um direito autônomo acabou por esvaziar seu núcleo essencial, formado pela privacidade, pela dignidade da pessoa humana, pela autodeterminação informativa e pelo livre desenvolvimento

da personalidade. Para piorar, a constitucionalização do Direito à Proteção de Dados no Brasil, além de incluí-lo como um direito de eficácia limitada, o posicionou em um caráter concorrencial com o Direito à Privacidade e com uma proteção mais frágil do que a que se tinha com a privacidade de eficácia plena, levantando questionamentos sobre a constitucionalidade da emenda n. 115/2022.

É possível observar que a ideia de que o Direito à Proteção de Dados é independente do Direito à Privacidade revela-se contraditória. Isso porque as violações de dados, especialmente as intervenções arbitrárias decorrentes da lei, só podem ser devidamente interpretadas à luz do Direito à Privacidade. A constatação demonstra que o Direito à Proteção de Dados pessoais carece de postulados próprios, mesmo dentro do âmbito da legalidade, permanecendo intrinsecamente dependente dos fundamentos estabelecidos pelo Direito à Privacidade.

O mencionado movimento transformou a proteção de dados em um conjunto de procedimentos a serem seguidos, sem uma preocupação substancial com a essência desse direito calcada na autodeterminação informativa efetiva e, sobretudo, com a garantia do Direito à Privacidade. Enquanto o *Datenschutz* destacava a necessidade de que o uso dos dados, desde o início até o final do tratamento, ocorresse em conformidade com os interesses originais do titular, atualmente, observa-se um desvio interpretativo em relação à proteção de dados e à privacidade, que deixaram de ser compreendidos como direitos fundamentais do indivíduo para se tornarem direitos negociáveis.

Tal transformação é evidenciada pela banalização do consentimento informado, considerando que o titular do direito, ao confrontar os termos e condições apresentados, geralmente não possui capacidade técnica para avaliar as condições, nem tempo suficiente para ler os extensos documentos. Além disso, há um fator determinante: o interesse predominante em usufruir da tecnologia frequentemente se sobrepõe à preocupação em proteger suas informações pessoais. Assim, vislumbra-se um apagar das luzes da proposta inicial do *Datenschutz,* que prejudica gravemente a autodeterminação informativa e a efetividade do Direito à Privacidade. No contexto da transferência internacional de dados, existem diversas deficiências que evidenciam a falta de comprometimento, tanto da lei quanto do regulamento, em tornar a proteção dos dados dos titulares verdadeiramente efetiva. As falhas se manifestam, principalmente, pela ausência de iniciativas voltadas à resolução de

dilemas jurisdicionais, à consolidação de uma soberania regulatória e à promoção de uma política consistente de proteção de dados.

II. Um fluxo internacional de dados precisa ser regulado. A privacidade *in abstrato* (*actio popularis*) no contexto do Big Data: As hipóteses previstas na LGPD e no regulamento instituído pela Resolução nº 19/2024 da ANPD tratam a transferência internacional de dados como um fenômeno estável e pontual. O enfoque, no entanto, desconsidera o expressivo descontrole informacional característico da atualidade, amplamente denominado, em termos sociológicos e tecnológicos, como *Big Data*. Um fenômeno que se aproveita, principalmente, do estado anárquico do ambiente digital, onde as fronteiras são ignoradas, para possibilitar evasões às normas legais.

Nessa senda, a regulação brasileira adota soluções tradicionais para lidar com problemas novos e não convencionais. Quando a violação da privacidade ocorre por meio do *Big Data* e da economia de vigilância de maneira sistemática e generalizada, como o indivíduo pode reivindicar um dano personalíssimo? A coletivização das violações torna essas práticas absolutamente abstratas e impessoalizadas, ofuscando os interesses individuais em prol de interesses considerados gerais. Assim, a abordagem tradicional de violação pelos critérios *ratione personae* e *ratione materiae* se mostra incapaz de efetivar o Direito à Privacidade.

É, portanto, essencial que a ANPD estabeleça expressamente a possibilidade de o sujeito, no âmbito da transferência internacional de dados, apresentar uma petição *in abstrato*, considerando apenas a probabilidade de ocorrência de um dano, e que seja possível pleitear interesses coletivos junto à ANPD. A previsão deve levar em conta a vulnerabilidade do sujeito e a generalização e sistematização das violações na contemporaneidade. Além disso, é fundamental que a ANPD assuma um papel ativo e fiscalizador nas transferências internacionais de dados, reconhecendo-as como fenômenos amplamente descontrolados, e promovendo auditorias – o regulamento e a LGPD não preveem a possibilidade de revisão das decisões da ANPD, o que contrasta com o artigo 45 do GDPR – e investigações sobre violações de dados de forma coletiva – *actio popularis*. A ausência dessas medidas compromete gravemente a efetividade do direito à privacidade no contexto da transferência internacional de dados pessoais.

III. Sísifo é jurista? O kafkiano labirinto procedimental e os Direitos condenados ao fracasso: No mito de Sísifo, ele é condenado a um trabalho eterno, cujo método inevitavelmente o conduz ao fracasso, forçando-o a repetir a tarefa incessantemente. Não adianta estabelecer uma série de procedimentos se, ao segui-los, a proteção de dados e, em especial, o direito à privacidade continuarem sendo sistematicamente violados.

Em uma perspectiva kafkiana, não basta que um processo exista; ele precisa ser humano, efetivo e transparente. No final das contas, toda regulação deve nascer com a coragem de ser verdadeiramente efetiva. No caso da transferência internacional de dados, seu objetivo principal deve ser o compromisso genuíno com a proteção da privacidade.

Na União Europeia, há o entendimento de que as hipóteses de transferência internacional de dados oferecem, entre si, níveis distintos de proteção de dados pessoais, sendo uma mais seguras do que outras. Isso fica claro nas hipóteses de derrogações aplicáveis a situações específicas, cuja qual deve ser sempre analisada em caráter *ultima ratio,* quando nenhuma das anteriores for aplicável. No caso brasileiro, esse caráter não fica evidente, de modo que não é preciso utilizá-las em *ultima ratio*.

Ademais, a Lei Geral de Proteção de Dados, distintamente do art. 48 do GDPR, não possui um estatuto de bloqueio. Dito isso, a regulação brasileira não protege o espaço jurídico nacional contra intromissões de outras jurisdições. Assim, ao escolher não exercer soberania regulatória, o Brasil permite, no âmbito da proteção de dados, que outras jurisdições decidam sobre dados em território nacional, desprotegendo o titular em um contexto internacional. Assim, mais uma vez, o regulador brasileiro deixa de se atentar para uma aspecto procedimental imprescindível, porque tem impactos substanciais sobre a proteção da privacidade dos titulares contra intervenções estrangeiras.

Distintamente do art. 27 do GDPR, o Brasil não exige que processadores ou controladores de dados localizados fora do território nacional designem um representante legal no país. A ausência dessa previsão na LGPD dificulta a responsabilização de agentes internacionais e estrangeiros, comprometendo a proteção da privacidade dos cidadãos brasileiros.

Além disso, a lei cria um incentivo perverso para as empresas de tecnologia, ao tornar mais vantajoso não designar um representante legal no Brasil. Isso ocorre porque o custo de violar dados pessoais sem ser responsabilizado é inferior ao de garantir, de forma privada, a ampliação da proteção da lei, ao constituir um representante legal no país – mesmo não sendo obrigatório – e, consequentemente, estar sujeito a penalidades. Assim, a LGPD, ao lidar com a transferência internacional de dados pessoais, acaba, paradoxalmente, promovendo o seu próprio descumprimento.

Em continuidade, não há no regulamento da ANPD, a obrigação de promover a revisão periódica da permissão para transferência internacional de dados. Assim, caso seja permitida a transferência de dados para determinado agente, ele certamente não terá o compromisso de manter o padrão de privacidade ativo, já que estará ciente que a ANPD não promoverá revisão periódica da sua decisão. O GDPR é distinto, e promove a revisão periódica, com fundamento no art. 45 do GDPR, no mínimo, a cada 04 (quatro) anos. Assim, o titular do dados não tem garantias de que sua privacidade continuará sendo protegida após o ato de autorização ANPD e o agente de tratamento terá a certeza da impunidade. Logo, um instrumento de proteção substancial da privacidade na transferência internacional de dados acaba sendo ignorado.

A ANPD já previu a revisão das decisões apenas dos processos que resultem em sanção, conforme os arts. 68 e 69 da Resolução n. 01/2021. No entanto, não há qualquer previsão específica no regulamento de transferência internacional de dados relacionada a revisão das decisões.

Por fim, a Lei Geral de Proteção de Dados Pessoais e o regulamento de transferência internacional de dados (resolução n. 19/2024, da ANPD), não se preocupam em estabelecer, de forma robusta, o problema da jurisdição, que é o principal e mais cristalino problema envolvendo a transferência internacional de dados. A ausência de estatuto de bloqueio e de disposições expressas nesse sentido, evidenciam o descompromisso do país na matéria e a evidente escolha de, em matéria de privacidade, não exercer soberania regulatória. Dito isso, o Brasil assume seu papel como um país que deve ser considerado um paraíso de dados.

Em suma, a inexistência de mecanismos como o estatuto de bloqueio, a ausência de exigência de representantes legais no território nacional para agentes

estrangeiros, a falta de previsão de revisões periódicas das autorizações para transferências e a negligência em enfrentar as imbricações jurisdicionais indicam que a regulação brasileira opta por uma abordagem permissiva e insuficiente. As lacunas não apenas desprotegem os titulares brasileiros contra intervenções externas, mas também criam incentivos para o a violação dos direitos dos titulares. Ao evitar enfrentar com coragem os problemas da soberania regulatória e ao ignorar a imprescindibilidade de construir instrumentos efetivos de proteção, o Brasil se posiciona como um território permissivo para o trânsito decontrole informacional.

Em conclusão, sem ajustes profundos e uma revisão substancial de sua abordagem, a regulação da transferência internacional de dados no Brasil continuará a falhar em cumprir seu propósito fundamental, perpetuando a metáfora do trabalho de Sísifo, onde esforços procedimentais são eternos, mas nunca alcançam resultados concretos.

IV. A inobservância da relevância Internacional do Direito à Privacidade: Ao longo do capítulo 03, foi possível identificar a relevância internacional do Direito à Privacidade. No entanto, a ausência de uma política robusta em sua defesa, somada às críticas apresentadas e à falta de obrigatoriedade para a realização de estudos de impacto à privacidade nas transferências internacionais de dados, evidencia como esse direito permanece inefetivo. Tal inefetividade resulta da priorização de um direito fundamental do mercado como nova referência para a proteção de dados. Assim, o descaso observado no regulamento brasileiro e na LGPD revela não apenas uma falta de compromisso em cumprir o mandamento constitucional, mas também uma negligência em atribuir ao Direito à Privacidade a devida relevância no cenário internacional.

VII. Sem interoperabilidade regional: A Lei Geral de Proteção de Dados Pessoais (LGPD) e o Regulamento de Transferência Internacional de Dados demonstram uma falta de preocupação com fatores econômicos, regionais, locais, culturais e políticos característicos do contexto em que o Brasil está inserido. Não há esforços regulatórios significativos para estabelecer parcerias, harmonizar entendimentos ou promover a noção brasileira de proteção de dados junto a outros países latino-americanos.

Este trabalho destaca avanços relevantes no direito latino-americano, como a separação entre transmissão internacional de dados e transferência internacional de

dados, adotada no México e na Colômbia, que atribui diferentes níveis de responsabilidade aos agentes envolvidos. A falta de uma perspectiva regional no regulamento brasileiro impede a incorporação de disposições importantes como essas, que poderiam enriquecer o marco regulatório nacional.

Além disso, o regulamento para transferência internacional de dados poderia ser uma oportunidade para instituir um conselho ou observatório de Direito à Proteção de Dados na América Latina, promovendo a integração e a cooperação regional. Um marco regulatório que ignora a realidade cultural, econômica e política mais próxima de sua tutela jurisdicional compromete a proteção da privacidade de seus titulares, desconsiderando as particularidades regionais e deixando de fortalecer a proteção de dados.

Distintamente do que propõe Guadamuz (2004), não se pretende, com essas conclusões, afirmar de forma preconceituosa que o Direito Brasileiro é deficiente por não se alinhar ao padrão europeu. Os Estados Unidos adotam um modelo jurídico baseado não em direitos, mas em danos e, ainda assim, não são alvo de críticas acadêmicas com a mesma intensidade que os países latino-americanos, incluindo o Brasil, quando divergem do Direito Europeu.

Também não se afirma que o padrão europeu deva ser ignorado. Ao contrário, deve ser considerado de forma neutra, como um entre diversos referenciais, sem ser tratado como superior. Todavia, é inteligível que a ausência de um representante legal dificulta a responsabilização, uma vez que a existência de um agente é essencial para que a responsabilidade possa ser atribuída. Da mesma forma, a ausência do Estatuto de Bloqueio prejudica a soberania de maneira evidente, pois não impede que jurisdições externas intervenham nos direitos dos titulares.

Após a apresentação das respostas ao problema de pesquisa, que confirmam a inefetividade do direito à privacidade, o próximo passo é propor direções para futuras para resolver as dificuldades externadas acima.

É necessário que a LGPD seja revisada para estabelecer de forma clara que as hipóteses de derrogações — exceções aplicáveis a situações específicas — devem ser utilizadas apenas em caráter de *ultima ratio*, ou seja, quando não houver outra alternativa viável. Atualmente, a lei não explicita esse requisito, o que permite que tais exceções sejam aplicadas sem a devida análise de necessidade e proporcionalidade. A citada omissão pode resultar em abusos e no enfraquecimento

da proteção de dados, indo contra o princípio de que derrogações devem ser medidas excepcionais e justificadas.

A LGPD apresenta uma falha crítica que demanda intervenção legislativa: a falta de um “estatuto de bloqueio”, nos moldes do art. 48 do GDPR, para evitar que o cumprimento de obrigações legais ou regulatórias (art. 7º, II, da LGPD) seja utilizado como justificativa para transferências internacionais de dados que submetam informações pessoais a jurisdições estrangeiras. Essa omissão abre espaço para que normas de outros países se sobreponham à legislação brasileira, gerando conflitos jurisdicionais e comprometendo a proteção de dados no Brasil. A criação de um estatuto de bloqueio é, portanto, essencial para assegurar que a base legal do cumprimento de obrigações não seja instrumentalizada para transferências que violem a soberania nacional ou exponham dados a riscos desnecessários.

A distinção entre “transferência internacional de dados” e “transmissão internacional de dados pessoais” é interessante e merece revisão pelo legislador brasileiro. Baseada no controle e na finalidade do tratamento, a diferenciação poderia ser incorporada à LGPD para vislumbrar novas formas de envio de dados, que geram níveis distintos de responsabilidade. Enquanto a transferência internacional envolve a delegação do controle sobre os dados a uma entidade autônoma, a transmissão internacional mantém o poder decisório com o controlador original, limitando-se à execução técnica por parte do processador. A distinção reflete graus variados de risco e responsabilidade, exigindo medidas específicas para cada cenário. A revisão desse conceito pela legislação brasileira poderia aprimorar a proteção de dados, adaptando-a às complexidades do fluxo internacional de informações.

O poder legislativo deve incluir na LGPD a obrigatoriedade de que empresas estrangeiras ou internacionais que processem dados de cidadãos brasileiros designem um representante legal no Brasil. A obrigatoriedade seria de grande valia para assegurar a responsabilização efetiva desses agentes em casos de transferência internacional de dados, além de facilitar os trabalhos da Autoridade Nacional de Proteção de Dados (ANPD).

É fundamental que o poder legislativo promova alterações na LGPD para instituir a obrigatoriedade de revisões periódicas nas autorizações de transferência internacional de dados, à semelhança do previsto no artigo 45 do GDPR, que

estabelece um prazo mínimo de quatro anos para reavaliações. A falta dessa previsão na legislação brasileira permite que os agentes de tratamento descumpram compromissos após a concessão inicial da autorização, comprometendo a proteção contínua dos dados. A implementação de revisões regulares asseguraria que as transferências internacionais mantenham conformidade com padrões atualizados de privacidade, reforçando a confiança dos titulares de dados e coibindo práticas negligentes.

A Autoridade Nacional de Proteção de Dados (ANPD) deve instituir um observatório do Direito na América Latina, com o objetivo de monitorar e analisar as práticas e regulamentações de proteção de dados na região, responsável pela emissão de relatórios periódicos, que mapeariam tendências, desafios e boas práticas em matéria de privacidade e segurança de dados. A iniciativa não apenas fortaleceria a cooperação regional, mas também forneceria subsídios para a ANPD aprimorar suas políticas e alinhá-las aos padrões internacionais, promovendo maior harmonização e eficácia na proteção de dados pessoais em nível latino-americano.

A ANPD e o Legislador devem compreender o fluxo internacional de dados não como um evento pontual ou isolado, mas como parte do descontrole informacional característico do Big Data, em que informações são coletadas, processadas e compartilhadas em escala global e contínua. A complexidade desse cenário exige uma revisão da LGPD e a adoção de regulamentos com dimensões inovadoras, capazes de enfrentar os desafios do ambiente digital atual. É necessário criar mecanismos que vão além da abordagem tradicional, como a implementação de padrões de responsabilização proporcional, a promoção de tecnologias de privacidade por design e a adoção de modelos de governança que garantam transparência e controle efetivo aos titulares de dados. Somente com uma abordagem atualizada e proativa será possível resolver os problemas decorrentes do fluxo internacional de dados e assegurar a proteção dos direitos dos cidadãos brasileiros no cenário global.

Ao poder executivo, cabe medir esforços para a formulação de acordos regionais na América Latina, com o objetivo de estabelecer maior interoperabilidade regional em matéria de transferência internacional de dados. A criação de um marco comum de proteção de dados na região fortaleceria a cooperação internacional,

reduziria conflitos jurisdicionais e ampliaria a segurança jurídica para empresas, governos e cidadãos.

É imprescindível que os tribunais não adotem uma interpretação procedimentalista da Emenda Constitucional 115/2022, assegurando que o direito à proteção de dados seja harmonizado com princípios como, a privacidade, a proporcionalidade e a dignidade da pessoa humana, conforme já vem sendo feito pelo STF. Ao estavelecer uma perspectiva integrada, há o fortalecimento da efetividade da proteção de dados, garantindo que sua aplicação transcenda formalidades e promova, de maneira substantiva, a defesa dos direitos fundamentais dos cidadãos.

Os poderes Executivo, Legislativo e Judiciário precisam estudar e refletir de forma conjunta sobre como exercer, de maneira equilibrada, as funções de jurisdição prescritiva, adjudicativa e executiva no tema “internet e jurisdição”. Somente com a colaboração entre os três poderes será possível enfrentar os desafios jurídicos e técnicos impostos pela internet.

Abaixo, sugere-se caminhos para novas investigações e temas relevantes para pesquisas futuras, que possam aprofundar a análise sobre a proteção do Direito à Privacidade no contexto da proteção de dados pessoais.

Este trabalho conclui que a perspectiva individualista para a privacidade não é efetiva, o que impõe, inevitavelmente, uma discussão sobre a perspectiva coletiva do direito à privacidade. Entretanto, surge mais uma questão: a privacidade de grupo inevitavelmente levará à supressão da autonomia individual. Assim, surge um paradoxo cuja solução tem um valor jurídico inestimável: qual dos ataques à autonomia dos sujeitos – seja pela via individualista do consentimento ou pela coletivização da privacidade – parece menos ofensiva.

Ademais, é preciso fazer um questionamento: quantos desses problemas são essencialmente jurídicos e o direito resolverá tudo? Se uma privacidade é violada porque uma tecnologia não foi projetada para proteger a privacidade, o problema é essencialmente do desenvolvimento tecnológico que não se importa com valores jurídicos consagrados e não um problema jurídico propriamente dito.

Assim, é necessário questionar a ausência de aplicação jurídica para que tecnologias sejam projetadas para não ofenderem direitos dos titulares ou direitos

coletivos. Logo, sugere-se uma revisão jusfilosófica que distinga quais problemas são verdadeiramente jurídicos.

Grande parte das dificuldades contemporâneas deve-se ao fato de as tecnologias serem tidas como incontestáveis, de modo que os juristas oferecem ataques epistemológicos constantes ao Direito. O Direito precisa se adequar às tecnologias, mas o inverso raramente ocorre. O Direito fica em segundo plano em relação à tecnologia.

Ao encerrar esta dissertação, é fundamental reafirmar que a proteção do direito à privacidade no contexto da transferência internacional de dados pessoais enfrenta dilemas profundos e multifacetados, que demandam uma revisão crítica e uma atuação coordenada entre os poderes Executivo, Legislativo e Judiciário. A análise realizada ao longo deste trabalho evidenciou que, embora a Lei Geral de Proteção de Dados (LGPD) e o regulamento da ANPD representem avanços significativos, ainda há lacunas e insuficiências que comprometem a efetividade da privacidade como direito fundamental. A ausência de mecanismos como o estatuto de bloqueio, a falta de revisões periódicas das autorizações de transferência e a negligência em relação à soberania regulatória são apenas alguns dos pontos críticos que precisam ser enfrentados com urgência.

Além disso, a dissertação destacou a necessidade de uma abordagem mais coletiva e regional para a proteção de dados, que leve em consideração as particularidades culturais, econômicas e políticas da América Latina. A criação de um observatório regional e a promoção de acordos de interoperabilidade são propostas que podem fortalecer a proteção da privacidade em um cenário globalizado e cada vez mais complexo. Por fim, é essencial que o Direito não apenas se adapte às tecnologias, mas também influencie seu desenvolvimento, garantindo que os valores jurídicos fundamentais, como a privacidade e a dignidade humana, sejam respeitados desde a concepção das inovações tecnológicas.

Em síntese, a efetiva proteção do direito à privacidade na transferência internacional de dados exige não apenas ajustes normativos, mas também uma mudança de paradigma que coloque os direitos fundamentais no centro das discussões sobre tecnologia e globalização. Este trabalho espera contribuir para essa reflexão, apontando caminhos que possam levar a uma regulação mais justa,

equilibrada e eficaz, capaz de garantir a privacidade como um direito inalienável em um mundo cada vez mais interconectado.

REFERÊNCIAS

ALBORNOZ, María Mercedes. Expansión del ámbito territorial de aplicación de la ley en materia de protección de datos personales:¿ Tendencia en América Latina?. Latin American Law Review, n. 9, p. 139-160, 2022.

ALHABABI, Hamad Hamed. Cross-Border Data Transfer between the gcc Data Protection Laws and the gdpr. Global Journal of Comparative Law, v. 13, n. 2, p. 178-200, 2024.

ÁLVAREZ-VALENZUELA, Daniel. La protección de datos personales en contextos de pandemia y la constitucionalización del derecho a la autodeterminación informativa. Revista chilena de derecho y tecnología, v. 9, n. 1, p. 1-4, 2020.

ANDREWS, Leighton. Facebook, The Media and Democray: Big Tech, Small State. Routledge Focus, 2020.

ANGARITA, Nelson Remolina; ZULUAGA, Luisa Fernanda Álvarez. Accountability Guide on Cross-border Transfers of Personal Data. 2019.

ANGARITA, Nelson Remolina. Aproximación Constitucional de la Protección de Datos Personales en Latinoamérica. Revista Internacional de Protección de Datos Personales, v. 13, 2012.

ASOCIACIÓN, POR LOS DERECHOS CIVILES. El Sistema de Protección de Datos Personales en América Latina: Oportunidades y Desafíos para los Derechos Humanos. Buenos Aires, Argentina: ADC, 2017.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Resolução CD/ANPD nº 1, de 28 de outubro de 2021. Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados. Diário Oficial da União: seção 1, Brasília, DF, 29 out. 2021. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no1-2021. Acesso em: 8 fev. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Resolução CD/ANPD nº 19, de 23 de agosto de 2024. Aprova o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais. Diário Oficial da União: seção 1, Brasília, DF, ano 162, n. 163, p. 123, 23 ago. 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: 8 fev. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Diário Oficial da União: seção 1, Brasília, DF, 28 jan. 2022. Disponível em: https://www.gov.br/anpd/pt-

br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022. Acesso em: 8 fev. 2025.

BAGHAI, Katayoun. Privacy as a human right: a sociological theory. Sociology, v. 46, n. 5, p. 951-965, 2012.

BELLI, Luca; DONEDA, Danilo. O que falta ao Brasil e à América Latina para uma proteção de dados efetiva? Como abordar parâmetros internacionais e reconhecer diferenças regionais? JOTA, 2021. Disponível em: https://www.jota.info/artigos/o-que-falta-ao-brasil-e-a-america-latina-para-uma-protecao-de-dados-efetiva. Acesso em: 30 jan. 2025.

BELLI, Luca; NOUGRÈRES, Ana Brian; MENDOZA ISERTE, Jonathan; PALAZZI, Pablo Andrés; REMOLINA ANGARITA, Nelson. Transferência Internacional de Dados Pessoais na América Latina: rumo à harmonização de normas. Rio de Janeiro: Lumen Juris, 2024.

BELTRÃO, Silvio Romero; MENEZES, Renata Oliveira Almeida. Evolução Histórica do Direito à Intimidade e os Desafios Contemporâneos para a Preservação do Paciente. Revista Jurídica Luso Brasileira, n. 3, 2018.

BELTRÃO, Silvio Romero. Direito da personalidade–natureza jurídica, delimitação do objeto e relações com o direito constitucional. RIDB, Porto, ano, v. 2, n. 1, p. 203-228, 2013.

BENTZEN, Heidi Beate; OLAV, Hilde Kvammen; URSIN, Giske. Maximizing the GDPR potential for data transfers: first in Europe. The Lancet Regional Health–Europe, v. 27, 2023.

BERTONI, Eduardo. Convention 108 and the GDPR: Trends and perspectives in Latin America. Comput. Law Secur. Rev., v. 40, p. 105516, 2021.

BIONI, Bruno Ricardo; ALVES, Fabrício Mota. A importância da PEC de proteção de dados mesmo após o histórico julgamento do STF. Coluna Jota, v. 16, 2020.

BIONI, Bruno Ricardo; DA SILVA, Paula Guedes Fernandes; MARTINS, Pedro Bastos Lobo. Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. Cadernos Técnicos da CGU, v. 1, 2022.

BIONI, Bruno Ricardo. A produção normativa a respeito da privacidade na economia da informação e do livre fluxo informacional transfronteiriço. Direitos e novas tecnologias: XXIII Encontro Nacional do Conpedi, p. 59-82, 2014.

BIONI, Bruno Ricardo. Autodeterminação informacional: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. 2016. Dissertação (Mestrado em Direito) –

Faculdade de Direito, Universidade de São Paulo, São Paulo, 2016.

BIONI, Bruno. Ecology: an intelligent narrative for the protection of personal data in smart cities. In: ICT ELECTRONIC GOVERNMENT SURVEY 2017: ARTICLES, p. 191-198. Disponível em: https://brunobioni.com.br/wp-content/uploads/2021/10/Ecology-Bioni.pdf. Acesso em: 11 jan. 2025.

BORGES, Roxana Cardoso Brasileiro. Direitos de Personalidade e Autonomia Privada. 2ª Ed. Editora Saraiva, 2007.

BOSHE, Patricia. Data privacy law: an international perspective. Information & Communications Technology Law, v. 24, n. 1, p. 118-120, 2015. Disponível em: https://doi.org/10.1080/13600834.2014.996324. Acesso em: 20 de fev. de 2025.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Planalto, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 24 out. 2022.

BRASIL. Agência Nacional de Proteção de Dados. 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: 10 jan. 2025.

BRASIL. Lei Federal nº 13.709, de 14 de Agosto de 2018. Dispõe Sobre a Lei Geral de Proteção de Dados Pessoais. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/l13709.htm>. Acesso em 04 de Agosto de 2022.

BRÄUTIGAM, Tobias. The land of confusion: international data transfers between Schrems and the GDPR. Data Protection, Privacy and European Regulation in the Digital Age’(Helsinki, 2016), Helsinki Legal Studies Research Paper, v. 46, 2016.

BRKAN, Maja. Privacy, data protection and the role of European Courts: Towards judicialisation and constitutionalisation of European privacy and data protection framework. In: GONZÁLEZ FUSTER, Gloria; VAN BRAKEL, Rosamunde; DE HERT, Paul (org.). Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics. Edward Elgar, 2022. p. 274-302.

BROWNSWORD, Roger. Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul; DE TERWANGNE, Cecile; NOUWT, Sjaak (org.). Reinventing Data Protection?. Springer, 2009. p. 83-110.

BÚRCA, Gráinne de. Introduction to the Symposium on the GDPR and International Law. Cambridge University Press, 2020.

BYGRAVE, Lee A.; SCHARTUM, Dag Wiese. Consent, Proportionality and Collective Power. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul; DE TERWANGNE, Cecile; NOUWT, Sjaak (org.). Reinventing Data Protection?. Springer, 2009. p. 157-173.

CANCELIER, Mikhail Vieira de Lorenzi. O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. Sequência (Florianópolis), p. 213-239, 2017.

CANOTILHO, J.J. GOMES. Civilização do Direito Constitucional ou Constitucionalização do direito Civil? A Eficácia dos Direitos Fundamentais na Ordem Jurídico-Civil no Contexto do Direito Pós-Moderno. In Eros Roberto Grau e Willis Santiago Guerra Filho (Org.). Direito Constitucional: Estudos em homenagem a Pulo Bonavides. Malheiros, 2003.

CARRASQUILLA, L. Personal data protection in Latin America: retention and processing of personal data in the Internet sphere. In: TOWARDS AN INTERNET FREE OF CENSORSHIP: PROPOSALS FOR LATIN AMERICA. Buenos Aires: Centro de Estudios en Libertad de Expresion y Acceso a la Informacion (CELE), 2012.

CARRASQUILLA, Lorenzo Villegas. Protección de Datos Personales em América Latina: Retención y Tratamiento de Datos Personales en el Mundo de Internet. In: BERTONI, Eduardo. Hacia una Internet Libre de Censura: Propuestas para América Latina. Buenos Aires: Universidade de Palermo, 2012, p. 125-164.

CARVALHO, Luis Gustavo Grandinetti de; CARVALHO, D. E. Direito à privacidade. Revista da EMERJ, v. 1, n. 2, 1998.

CATE, Fred H. et al. The end of the beginning. 2012.

CATE, Fred H.; MAYER-SCHÖNBERGER, Viktor. Notice and consent in a world of Big Data. International Data Privacy Law, v. 3, n. 2, p. 67-73, 2013.

CELLI JUNIOR, Umberto. Tecnologias digitais e o comércio de bens e serviços na OMC/Digital. Revista de Direito Internacional, v. 17, n. 1, 2020.

CHIAPPETTA, Aline Holanda. Transferências transatlânticas de dados pessoais na era pós-Snowden à luz do Regulamento Geral sobre a Proteção de Dados. 2018. 118 f. Dissertação (Mestrado em Ciências Jurídico-Empresariais) – Faculdade de Direito, Universidade de Coimbra, Coimbra, 2018.

COCHE, Eugénie; KOLK, Ans; OCELÍK, Václav. Unravelling cross-country regulatory intricacies of data governance: the relevance of legal insights for digitalization and international business. Journal of International Business Policy, v. 7, n. 1, p. 112-127, 2023.

COLÔMBIA. Decreto nº 1377, de 27 de junho de 2013. Regulamenta parcialmente a Lei Estatutária nº 1581 de 2012 sobre proteção de dados pessoais. Disponível em:

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646. Acesso em: 10 jan. 2025.

COLÔMBIA. Lei Estatutária nº 1581, de 17 de outubro de 2012. Dispõe sobre a proteção de dados pessoais. Disponível em: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981. Acesso em: 10 jan. 2025.

COLÔMBIA. Superintendência de Indústria e Comércio. Circular nº 05, de 10 de agosto de 2017. Publicada no Diário Oficial nº 50321, em 10 de agosto de 2017. Disponível em: https://www.sic.gov.co/noticias-boletin-juridico-agosto-2017/circular-no-05-del-10-de-agosto-de-2017-publicada-en-el-diario-oficial-no-50321-del-10-de-agosto-de-2017. Acesso em: 10 jan. 2025.

CONTRERAS, Pablo. El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena. Estudios constitucionales, v. 18, n. 2, p. 87-120, 2020. CORRÊA, André Luiz da Costa. A constitucionalização dos direitos à intimidade e à vida privada. São Paulo, SP: PUC, 2005.

COSTA FILHO, Venceslau Tavares. Pode falar-se em um direito civil pós-moderno? Crítica ao romantismo renovado no direito civil. Revista Jurídica Luso-brasileira, ano 5 (2019), n. 3, p. 1.823-1.836.

COSTA, José Américo Martins da. Releitura constitucional no conflito entre os direitos fundamentais na proteção conferida à privacidade e o acesso à informação. 2018. Tese de Doutorado.

COULDRY, N.; MEJIAS, U. A. Colonialismo de Datos: Repensando la Relación de los Datos Masivos con el Sujeto Contemporáneo. Virtualis: Revista de cultura digital, v. 10, n. 18, p. 78-97, 20 maio 2019a. Disponível em: http://www.revistavirtualis.mx/index.php/virtualis/article/view/289. Acesso em: 11 jun. 2022.

COULDRY, N.; MEJIAS, U. A. The Costs of Connection: How Data is Colonizing Human Life and Appropriating it for Capitalism. Stanford: Stanford University Press, 2019b.

COULDRY, Nick. Colonialismo de Dados e Esvaziamento da Vida Social Antes e Pós Pandemia De Covid-19. Homo Digitalis: A Escalada da Algoritimização da Vida, 2022.

DA SILVA, José Afonso. Aplicabilidade das normas constitucionais. Editora Revista dos Tribunals, 1982.

DA SILVA, Virgílio Afonso. O conteúdo essencial dos direitos fundamentais e a eficácia das normas constitucionais. Revista de direito do Estado, Rio de Janeiro, v. 4, p. 23-51, 2006.

DE ÁVILA CHAGAS, Rossana Gleucy; CARVALHO, Márcio Matias. DIREITO DE PRIVACIDADE NO BRASIL. ANAIS WIDaT 2018, v. 58.

DE ÁVILA NEGRI, Sergio Marcos Carvalho; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. A normatividade dos dados sensíveis na lei geral de proteção de dados: ampliação conceitual e proteção da pessoa humana. Revista de Direito, Governança e Novas Tecnologias, v. 5, n. 1, p. 63-85, 2019.

DE HERT, P.; GUTWIRTH, S. Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul; DE TERWANGNE, Cecile; NOUWT, Sjaak (org.). Reinventing Data Protection?. Springer, 2009. p. 3-44.

DE TERWANGNE, Cecile. Is a Global Data Protection Regulatory Model Possible?. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul; DE TERWANGNE, Cecile; NOUWT, Sjaak (org.). Reinventing Data Protection?. Springer, 2009. p. 175-189.

DIAS, Clara Angélica Gonçalves Cavalcanti; DA ANUNCIAÇÃO MELO, Bricio Luis. A autodeterminação informativa como manifestação do direito à privacidade. Revista de Direito Civil Contemporâneo-RDCC (Journal of Contemporary Private Law), v. 37, p. 51-75, 2023.

DIGGELMANN, Oliver; CLEIS, Maria Nicole. How the right to privacy became a human right. Human Rights Law Review, v. 14, n. 3, p. 441-458, 2014.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 2006.

DWORKIN, Ronald. A matter of principle. Harvard University Press, 1985.

DWORKIN, Ronald. Justice for hedgehogs. Harvard University Press, 2011.

DWORKIN, Ronald. Law’s empire. Harvard University Press, 1986.

ESPEEL, Thomas; COLSON, Eléonore; CRUQUENAIRE, Alexandre. International data transfers under GDPR: applicable requirements and practical implementation. Le droit des affaires, n. 141, p. 19-41, 2022.

EVANGELISTA, Samuel Sampaio et al. Constitucionalismo digital: uma análise sobre o Estado e o direito fundamental da proteção de dados. Dissertação de Mestrado. Universidade Lusófona, 2021.

FINCK, Michèle; PALLAS, Frank. They who must not be identified—distinguishing personal from non-personal data under the GDPR. International Data Privacy Law, v. 10, n. 1, p. 11-36, 2020.

FORNASIER, Mateus de Oliveira; KNEBEL, Norberto Milton Paiva. O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados. Revista Direito e Práxis, v. 12, p. 1002-1033, 2021.

FRAGOSO, Suely; MALDONADO, Alberto Efendy. The Internet in Latin America. International Handbook of Internet Research, p. 201-215, 2010.

FRANCO, Carolina Mendes. A pessoa humana resumida a um dado corporal: considerações sobre o tratamento adequado aos dados biométricos. 2009. 121 f. Dissertação (Mestrado em Direito Civil Constitucional; Direito da Cidade; Direito Internacional e Integração Econômica; Direi) - Universidade do Estado do Rio de Janeiro, Rio de janeiro, 2009.

GENTILE, Giulia; LYNSKEY, Orla. Deficiente por design? A aplicação transnacional do GDPR. International & Comparative Law Quarterly , v. 71, n. 4, p. 799-830, 2022.

GONZALBO, Fernando Escalante. El Derecho a la privacidad. Instituto Federal de Acceso a la Información y Protección de Datos, 2004.

GRAZZI, Matteo; VERGARA, Sebastián. Internet in Latin America: Who uses it?… and for what?. Economics of Innovation and New Technology, v. 23, n. 4, p. 327-352, 2013.

GUADAMUZ, Andrés. Habeas data vs. the European data protection directive. Journal of Information, Law & Technology, v. 3, 2004.

GUTIÉRREZ, Jesús María Prieto. Objeto y naturaleza jurídica del derecho fundamental a la protección de datos personales (y II). Boletín del Ministerio de Justicia, n. 1973, p. 3317-3337, 2004.

HEUVEL, Karlijn van den; HOBOKEN, Joris van. The justiciability of data privacy issues in Europe and the US. In: GONZÁLEZ FUSTER, Gloria; VAN BRAKEL, Rosamunde; DE HERT, Paul (Org.). Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics. Cheltenham: Edward Elgar Publishing, 2022. p. 73-108.

JULIUSSEN, Bjørn Aslak et al. The third country problem under the GDPR: enhancing protection of data transfers with technology. International Data Privacy Law, v. 13, n. 3, p. 225-243, 2023.

KALTMEIER, Olaf. Refeudalização e guinada à direita: desigualdade social e cultura política na América Latina. 1ª Edição. Editora Philos, 2020.

KIDWELL, Linda. GDPR Compliance in EU-US Data Transfers-Examining the impact of the EU Commission’s 2023 adequacy decision on surveillance risks. 2023.

KRAMCSAK, Pablo Rodrigo Trigo. Personal Data Protection and Data Transfer Regulation in Brazil. Brussels Privacy Hub Working Paper, vol. 10, n° 2, 2024.

KRAMER, Andreas. Jus Cogens and Privacy: A Critical Review of Internet Regulation and Personal Freedoms. 2024.

KUNER, Christopher et al. Data protection and humanitarian emergencies. International Data Privacy Law, v. 7, n. 3, p. 147-148, 2017.

KUNER, Christopher et al. If the legislature had been serious about data privacy. International Data Privacy Law, v. 9, n. 2, p. 75-77, 2019.

KUNER, Christopher et al. Internet Balkanization gathers pace: is privacy the real driver?. International Data Privacy Law, v. 5, n. 1, p. 1-2, 2015.

KUNER, Christopher et al. PRISM and privacy: will this change everything?. International Data Privacy Law, v. 3, n. 4, p. 217-219, 2013a.

KUNER, Christopher et al. Privacy—an elusive concept. International Data Privacy Law, v. 1, n. 3, p. 141-142, 2011.

KUNER, Christopher et al. The (data privacy) law hasn't even checked in when technology takes off. International Data Privacy Law, v. 4, n. 3, p. 175-176, 2014.

KUNER, Christopher et al. The business of privacy. International Data Privacy Law, v. 3, n. 2, p. 65-66, 2013b.

KUNER, Christopher et al. The challenge of ‘big data’for data protection. **International Data Privacy Law**, v. 2, n. 2, p. 47-49, 2012.

KUNER, Christopher et al. The extraterritoriality of data privacy laws—an explosive issue yet to detonate. International Data Privacy Law, v. 3, n. 3, p. 147-148, 2013.

KUNER, Christopher et al. The GDPR as a chance to break down borders. International Data Privacy Law, v. 7, n. 4, p. 231-232, 2017.

KUNER, Christopher et al. The global data protection implications of ‘Brexit’. International Data Privacy Law, v. 6, n. 3, p. 167-169, 2016.

KUNER, Christopher et al. The rise of cybersecurity and its impact on data protection. International Data Privacy Law, v. 7, n. 2, p. 73-75, 2017.

KUNER, Christopher. An international legal framework for data protection: Issues and prospects. Computer law & security review, v. 25, n. 4, p. 307-317, 2009b.

KUNER, Christopher. Article 44. General principle for transfers. In: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher (org.). The EU General Data

Protection Regulation (GDPR): A Commentary. Oxford: Oxford University Press, 2020a. p. 755-770.

KUNER, Christopher. Article 45. Transfers on the basis of an adequacy decision. In: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher (org.). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford: Oxford University Press, 2020b. p. 771-796.

KUNER, Christopher. Article 46. Transfers subject to appropriate safeguards. In: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher (org.). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford: Oxford University Press, 2020c. p. 797-812.

KUNER, Christopher. Article 47. Binding corporate rules. In: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher (org.). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford: Oxford University Press, 2020d. p. 813-824.

KUNER, Christopher. Article 48. Transfers or disclosures not authorised by Union law. In: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher (org.). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford: Oxford University Press, 2020e. p. 825-840.

KUNER, Christopher. Article 49. Derogations for specific situations. In: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher (org.). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford: Oxford University Press, 2020f. p. 841-856.

KUNER, Christopher. Article 50. International cooperation for the protection of personal data. In: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher (org.). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford: Oxford University Press, 2020g. p. 857-862.

KUNER, Christopher. Data protection law and international jurisdiction on the Internet (part 1). International Journal of Law and Information Technology, v. 18, n. 2, p. 176-193, 2010a.

KUNER, Christopher. Developing an Adequate Legal Framework for International Data Transfers. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul; DE TERWANGNE, Cecile; NOUWT, Sjaak (org.). Reinventing Data Protection?. Springer, 2009b. p. 263-273.

KUNER, Christopher. Global Data Transfers on the Internet: Lessons from the Ancient World. Available at SSRN 1445458, 2009a.

KUNER, Christopher. Lei de proteção de dados e jurisdição internacional na Internet (Parte 2). International Journal of Law and Information Technology , v. 18, n. 3, p. 227-247, 2010b.

KUNER, Christopher. Reality and illusion in EU data transfer regulation post Schrems. German Law Journal, v. 18, n. 4, p. 881-918, 2019.

KUNER, Christopher. Regulation of transborder data flows under data protection and privacy law: past, present, and future. TILT Law & Technology Working Paper, n. 016, 2010c.

KUNER, Christopher. Territorial scope and data transfer rules in the GDPR: Realising the EU’s ambition of borderless data protection. University of Cambridge Faculty of Law Research Paper, n. 20, 2021.

KUNER, Christopher. The European Commission's proposed data protection regulation: A copernican revolution in European data protection law. Bloomberg BNA Privacy and Security Law Report (2012) February, v. 6, n. 2012, p. 1-15, 2012.

KUNER, Christopher. The European Union and the search for an international data protection framework. Groningen Journal of International Law, v. 2, n. 2, p. 55-71, 2014.

KUNER, Christopher. The Internet and the global reach of EU law. The Internet and the global reach of EU law’, in: Marise Cremona and Joanne Scott (eds.), EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law, p. 112-145, 2017.

KURAT, Jensen. Evaluating Jus Cogens Norms in Digital Privacy: Balancing Internet Governance and Personal Liberties. 2023a.

KURAT, Jensen. Jus Cogens Norms and Digital Privacy: Evaluating Internet Governance and the Balance of Personal Liberties. 2023b.

LAFER, Celso. A reconstrução dos direitos humanos: um diálogo com o pensamento de Hannah Arendt. Companhia das Letras, 1988.

LESSIG, Lawrence. Reading the constitution in cyberspace. Emory Lj, v. 45, p. 869, 1996.

LIMBERGER, Têmis. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. Novos Estudos Jurídicos, v. 14, n. 2, p. 27-53, 2009.

LINDERFALK, Ulf. The Source of Jus Cogens Obligations–How Legal Positivism Copes with Peremptory International Law. Nordic Journal of International Law, v. 82, n. 3, p. 369-389, 2013.

LUKÁCS, Adrienn. What is privacy? The history and definition of privacy. 2016.

MAGALHÃES, Brunno Roberto Araujo Lins; DE ANDRADE MATTIETTO, Leonardo. POLÍTICAS PÚBLICAS E O DIREITO A PROTEÇÃO DE DADOS: UMA ANÁLISE DA ADI Nº 6561/TO. Revista de Direito da Administração Pública, v. 1, n. 03, 2023.

MAGALHÃES, João; COULDRY, Nick. Gigantes da tecnologia estão usando esta crise para colonizar o Estado. Jacobin, 2020. Disponível em:< https://jacobin.com.br/2020/05/gigantes-da-tecnologia-estao-usando-esta-crise-paracolonizar-o-estado >. Acesso em: 18 de abril de 2024.

MAGALHÃES, João; COULDRY, Nick. Giving by taking away: Big tech, data colonialism and the reconfiguration of social good.International Journal of Communication, v. 15, p. 343-362, 2021.

MANTOVANI, Martina. Contractual obligations as a tool for international transfers of personal data under the GDPR. Available at SSRN 3522426, 2020.

MARELLI, Massimo. Transferring personal data to international organizations under the GDPR: an analysis of the transfer mechanisms. International Data Privacy Law, v. 14, n. 1, p. 19-36, 2023.

MASSON, Nathalia. Manual de Direito Constitucional. 8ª Ed. Editora Juspodivm, 2020.

MATTOO, Aaditya; MELTZER, Joshua P. International data flows and privacy: The conflict and its resolution. Journal of International Economic Law, v. 21, n. 4, p. 769-789, 2018.

MCCULLAGH, Karen. Protecting ‘privacy'through control of ‘personal'data processing: A flawed approach. In: Information Technology and Traditional Legal Concepts. Routledge, 2013. p. 13-24.

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. Revista Brasileira de Direito, v. 16, n. 1, p. 1-33, 2020.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. Pensar Revista de Ciências Jurídicas Universidade de Fortaleza (Unifor), Fortaleza, v. 25, n. 4, p. 1-18, 2020.

MENDES, Laura Schertel; DA FONSECA, Gabriel C. Soares. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. REI-Revista Estudos Institucionais, v. 6, n. 2, p. 507-533, 2020.

MENDES, Laura Schertel; RODRIGUES JR., Otavio Luiz; FONSECA, Gabriel Campos Soares da. O Supremo Tribunal Federal, a proteção constitucional dos dados pessoais e a positivação superveniente de um direito fundamental autônomo. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz; BIONI, Bruno (Org.). Tratado de proteção de dados pessoais. 2. ed. Rio de Janeiro: Forense, 2023. p. 61-71.

MENDONÇA, Fernanda Graebin. O direito à autodeterminação informativa: a (des) necessidade de criação de um novo direito fundamental para a proteção de dados pessoais no Brasil. SEMINÁRIO INTERNACIONAL DE DEMANDAS SOCIAIS E POLÍTICAS PÚBLICAS NA SOCIEDADE CONTEMPORÂNEA, v. 11, 2014.

MÉXICO. Constitución Política de los Estados Unidos Mexicanos. Disponível em: https://www.diputados.gob.mx/LeyesBiblio/pdf/1_310123.pdf. Acesso em: 10 jan. 2025.

MÉXICO. Federal Law of Protection of Personal Data in the Possession of Private Individuals. Disponível em: https://www.global-regulation.com/translation/mexico/560242/federal-law-of-protection-of-personal-data-in-the-possession-of-private-individuals.html. Acesso em: 10 jan. 2025.

MÉXICO. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México. Disponível em: https://www.congresocdmx.gob.mx/media/documentos/a8b6a4657686ea6f01e7a024377b814e0664d634.pdf. Acesso em: 10 jan. 2025.

MOEREL, Lokke; PRINS, Corien. Privacy for the homo digitalis: Proposal for a new regulatory framework for data protection in the light of Big Data and the internet of things. Available at SSRN 2784123, 2016.

MOEREL, Lokke. Binding corporate rules: corporate self-regulation of global data transfers. OUP Oxford, 2012.

MOEREL, Lokke. The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?. International Data Privacy Law, v. 1, n. 1, p. 28-46, 2011.

MOORE, Adam D. Defining privacy. Journal of Social Philosophy, v. 39, n. 3, p. 411-428, 2008.

NASCIMENTO, Reginaldo Felix. Sistema Latino-americano de Proteção de Dados Pessoais. MANRIQUE, Jorge Isaac Torres; CALGARO, Cleide; BRASIL, Deilton Ribeiro. Anais do VI Congresso de Direito e Inteligência Artificial. Skema Business School, 2023.

NETO, Eugênio Facchini. A constitucionalização do direito privado. Revista Iurisprudentia, v. 2, n. 3, 2013.

NISSIM, Kobbi; WOOD, Alexandra. Is privacy privacy?. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, v. 376, n. 2128, p. 20170358, 2018.

NOUGRÈRES, Ana Brian. Data Protection and Enforcement in Latin America and in Uruguay. Enforcing Privacy: Regulatory, Legal and Technological Approaches, p. 145-180, 2016.

OLDANI, Isabella. Exchanging and Protecting Personal Data across Borders: GDPR Restrictions on International Data Transfer. 2020. 410 f. Tese (Doutorado) – Università degli Studi di Trento, Trento, 2020.

OLIVEIRA, Júlia Carrijo de. A proteção de dados pessoais como garantia dos direitos fundamentais: as decisões de adequação são mecanismos de tutela efetiva do direito fundamental no que toca às transferências internacionais para países terceiros? 2024. 63 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Escola do Porto, Universidade Católica Portuguesa, Porto, 2024.

PEHLIVAN, Ceyhun Necati. Data Protection in Latin America: An Overview. Global Privacy Law Review, v. 2, n. 2, 2021.

PENEDO, Andrés Chomczyk. Enabling cross border open finance systems in Latin America: is consent enough to develop them?. International Review of Law, Computers & Technology, p. 1-21, 2024.

PETRY, Gabriel Cemin; HUPFFER, Haide Maria. O direito à proteção de dados pessoais: um estudo do panorama legislativo da América Latina. Revista Culturas Jurídicas, Ahead of Print, 2024.

PRAMESTI, Indriana; AFRIANSYAH, Arie. Extraterritoriality of data protection: GDPR and its possible enforcement in Indonesia. In: 3rd International Conference on Law and Governance (ICLAVE 2019). Atlantis Press, 2020. p. 83-94.

RAMIRO, Mónica Arenas. Data protection in Latin America. In: FUSTER, Gloria González; VAN BRAKEL, Rosamunde; DE HERT, Paul (orgs.). Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics. Cheltenham: Edward Elgar, 2022. p. 140-159.

RENGEL, Alexandra. Privacy as an international human right and the right to obscurity in cyberspace. Groningen Journal of International Law, v. 2, n. 2, 2014.

RENGEL, Alexandra. Privacy in the 21st Century. Martinus Nijhoff Publishers, 2013.

RODOTÀ, Stefano. Data Protection as a Fundamental Right. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul; DE TERWANGNE, Cecile; NOUWT, Sjaak (org.). Reinventing Data Protection?. Springer, 2009. p. 77-82.

ROESSLER, Beate. X—privacy as a human right. In: Proceedings of the Aristotelian Society. Oxford University Press, 2017. p. 187-206.

ROUVROY, Antoinette; POULLET, Yves. The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul; DE

TERWANGNE, Cecile; NOUWT, Sjaak (org.). Reinventing Data Protection?. Springer, 2009. p. 45-76.

RUBENFELD, Jed. The right of privacy. Harvard Law Review, p. 737-807, 1989.

RYNGAERT, Cedric; TAYLOR, Mistale. The GDPR as global data protection regulation?. 2020.

SANTOS, Luiza Mendonça da Silva Belo. Interoperabilidade em transferências internacionais de dados pessoais: uma análise crítica dos regimes jurídicos de proteção de dados do Brasil, Argentina, Uruguai e Colômbia. 2023. 196 f. Dissertação (Mestrado em Direito) – Universidade de Brasília, Faculdade de Direito, Programa de Pós-Graduação em Direito, Brasília, 2023.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental autônomo na Constituição Brasileira de 1988. Direitos fundamentais na perspectiva da democracia interamericana 2020/2021, 2021.

SCHREIBER, A. Direitos da personalidade. 3. ed. São Paulo: Atlas, 2014.

SILVA, A. Personal Data Protection and Online Services in Latin America. In: TOWARDS AN INTERNET FREE OF CENSORSHIP: PROPOSALS FOR LATIN AMERICA. Buenos Aires: Centro de Estudios en Libertad de Expresion y Acceso a la Informacion (CELE), 2012.

SILVA, Alberto J. Cerda. Protección de Datos Personales y Prestación de Servicios em Línea em América Latina. In: BERTONI, Eduardo. Hacia una Internet Libre de Censura: Propuestas para América Latina. Buenos Aires: Universidade de Palermo, 2012, p. 165-180.

SILVA, L. G. ; NASCIMENTO, R. Felix. ; ROSA, H. S. L. M. S. . Direito fundamental à proteção de dados pessoais: transferência internacional de dados, geopolítica e big data. In: XII Congresso Internacional do CONPEDI, 2023, Buenos Aires. Anais do XII Congresso Internacional do CONPEDI. Florianópolis ? SC: CONPEDI, 2023. p. 152-169.

SILVA, Lucas Gonçalves da; NASCIMENTO, Reginaldo Felix; COSTA, Camilla Ellen Aragão. Tributação e Novas Tecnologias. Revista Jurídica Luso-brasileira, ano 9, nº 5, 1573-1602, 2023.

SILVA, Lucas Gonçalves da; NASCIMENTO, Reginaldo Felix. (De)colonialidade digital e a airbnbinificação das cidades: repercussões sociais e jurídicas. Direito Público, v. 21, n. 109, 2024. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/7707. Acesso em: 7 fev. 2025.

SILVA, Lucas Gonçalves da; NASCIMENTO, Reginaldo Felix. A virtualização do discurso político na democracia brasileira. Contribuciones a Las Ciencias Sociales, v. 16, p. 4782- 4802, 2023a.

SILVA, Lucas Gonçalves da; NASCIMENTO, Reginaldo Felix. Colonialismo de dados: o apagar das vozes no conhecimento social.Revista de Direitos e Garantias Fundamentais, v. 24, n. 3, p. 73-105, 2023b.

SILVA, Lucas Gonçalves da; NASCIMENTO, Reginaldo Felix. Direito Internacional da Economia Digital: relações contratuais na internet e proteção jurídica do consumidor. Relações Internacionais no Mundo Atual, v. 4, n. 42, p. 789-803, 2024.

SLOOT, Bart van der. Legal fundamentalism: Is data protection really a fundamental right?. Data protection and privacy:(in) visibilities and infrastructures, p. 3-30, 2017a.

SLOOT, Bart van der. Privacy as virtue: Moving beyond the individual in the age of big data. (No Title), 2017b.

SUDA, Yuko. The politics of data transfer: transatlantic conflict and cooperation over data privacy. Routledge, 2017.

SULLIVAN, Clare. EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era. computer law & security review, v. 35, n. 4, p. 380-397, 2019.

SVANTESSON, Dan Jerker B. A “layered approach” to the extraterritoriality of data privacy laws. International Data Privacy Law, v. 3, n. 4, p. 278-286, 2013.

SVANTESSON, Dan Jerker B. Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation. International Data Privacy Law, v. 5, n. 4, p. 226-234, 2015.

SVANTESSON, Dan Jerker B. Solving the internet jurisdiction puzzle. Oxford University Press, 2017.

SVANTESSON, Dan. Enforcing privacy across different jurisdictions. In: WRIGHT, David; DE HERT, Paul (org.). Enforcing privacy: regulatory, legal and technological approaches. Springer, 2016. p. 195-222.

TERWANGNE, Cécile de. Privacy and data protection in Europe: Council of Europe’s Convention 108+ and the European Union’s GDPR. In: FUSTER, Gloria González; BRAKEL, Rosamunde Van; HERT, Paul De (orgs.). Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics. Cheltenham: Edward Elgar, 2022. p. 10-35.

THOMSON, Judith Jarvis. The right to privacy. Philosophy & Public Affairs, p. 295-314, 1975.

TRAN, Hiep. Briefing on Data Processing and International Data Transfer in Accordance with GDPR. Available at SSRN 3538643, 2020.

TUBARO, Paola. 9. La vie privée, un bien commun?. Regards croisés sur l’économie, v. 23, n. 2, p. 129-137, 2018.

TZANOU, Maria. Data protection as a fundamental right next to privacy?‘Reconstructing’a not so new right. International Data Privacy Law, v. 3, n. 2, p. 88-99, 2013.

UNIÃO EUROPEIA. General Data Protection Regulation (GDPR). Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Disponível em: https://gdpr-info.eu/. Acesso em: 10 jan. 2025.

VAN DOORN, Niels. A new institution on the block: On platform urbanism and Airbnb citizenship.New media & society, v. 22, n. 10, p. 1808-1826, 2020.

VERONESE, Alexandre et al. The concept of personal data protection culture from European Union documents: a “Brussels effect” in Latin America?. 2023a.

VERONESE, Alexandre et al. The influence of European Union personal data protection standards in Latin America from the perspective of social actors and Latin American authorities. 2023b.

VERONESE, Alexandre; IGREJA, Rebecca Lemos; SILVEIRA, Alessandra. Cultura, privacidade e proteção de dados pessoais na América Latina: Bases teóricas para uma pesquisa de campo e de documento de caráter internacional. Revista de Estudos Empíricos em Direito, v. 10, p. 1-44, 2023c.

VERONESE, Alexandre. Percepções sociais sobre inteligência artificial e proteção de dados pessoais na América Latina: usando pesquisa qualitativa de campo em perspectiva comparada. Cadernos do Programa de Pós-graduação em Direito – PPGDir, v. 18, n. 1, p. 47-48, 2023d.

WAGNER, Julian. The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?. International Data Privacy Law, v. 8, n. 4, p. 318-337, 2018.

WEEKS, James K. Comparative law of privacy. Clev.-Marshall L. Rev., v. 12, p. 484, 1963.

ZUBOFF, Shoshana. A Era do Capitalismo de Vigilância. 1ª Ed. Editora, 2021.

ZUBOFF, Shoshana. Big Other: Capitalismo de Vigilância e Perspectivas para uma Civilização de Informação. In: BRUNO, Fernanda et al (org.). Tecnopolíticas da Vigilância: Perspectiva da Margem. 1ª Ed. Boitempo, 2015, 17-68.