

UNIVERSIDADE FEDERAL DA PARAÍBA – UFPB

CENTRO DE CIÊNCIAS JURÍDICAS – CCJ

COORDENAÇÃO DO CURSO DE DIREITO – CAMPUS JOÃO PESSOA

COORDENAÇÃO DE MONOGRAFIA

BEATRIZ BARROS DE MORAIS

SOBERANIA DIGITAL E OS LIMITES DA FISCALIZAÇÃO: A APLICAÇÃO DA LGPD E OS DESAFIOS DA ANPD FRENTE À TRANSFERÊNCIA INTERNACIONAL DE DADOS POR REDES SOCIAIS ESTRANGEIRAS

JOÃO PESSOA

2026

BEATRIZ BARROS DE MORAIS

SOBERANIA DIGITAL E OS LIMITES DA FISCALIZAÇÃO: A APLICAÇÃO DA LGPD E OS DESAFIOS DA ANPD FRENTE À TRANSFERÊNCIA INTERNACIONAL DE DADOS POR REDES SOCIAIS ESTRANGEIRAS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito de João Pessoa do Centro de Ciências Jurídicas da Universidade Federal da Paraíba como requisito parcial da obtenção do grau de Bacharel em Direito.

Orientadora: Dr.ª Lorena de Melo Freitas

JOÃO PESSOA

2026

Catalogação na publicação
Seção de Catalogação e Classificação

M827s Morais, Beatriz Barros de.
Soberania digital e os limites da fiscalização: a aplicação da LGPD e os desafios da ANPD frente à transferência internacional de dados por redes sociais estrangeiras / Beatriz Barros de Morais. - João Pessoa, 2026.
56 f. : il.

Orientação: Lorena De Melo Freitas.
TCC (Graduação) - UFPB/JP.

1. Soberania digital. 2. LGPD. 3. ANPD. 4. Transferência internacional de dados. 5. Fiscalização. I. Freitas, Lorena De Melo. II. Título.

UFPB/CCJ CDU 34

Elaborado por LUCIMARIO DIAS DOS SANTOS - CRB-15/645

BEATRIZ BARROS DE MORAIS

SOBERANIA DIGITAL E OS LIMITES DA FISCALIZAÇÃO: A APLICAÇÃO DA LGPD E OS DESAFIOS DA ANPD FRENTE À TRANSFERÊNCIA INTERNACIONAL DE DADOS POR REDES SOCIAIS ESTRANGEIRAS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito de João Pessoa do Centro de Ciências Jurídicas da Universidade Federal da Paraíba como requisito parcial da obtenção do grau de Bacharel em Direito.

Orientadora: Dr.ª Lorena de Melo Freitas

DATA DA APROVAÇÃO: 27 DE MARÇO DE 2026

BANCA EXAMINADORA:

Assinado digitalmente na ZapSign por
LORENA DE MELO FREITAS
Data: 10/04/2026 21:29:47.917 (UTC-0300)

Prof.ª Dr.ª LORENA DE MELO FREITAS
(ORIENTADORA)

Assinado digitalmente na ZapSign por
JONÁBIO BARBOSA DOS SANTOS
Data: 10/04/2026 21:52:29.179 (UTC-0300)

Prof. Dr. JONÁBIO BARBOSA DOS SANTOS
(AVALIADOR)

Assinado digitalmente na ZapSign por
IAGO MORAIS DE OLIVEIRA MOURA
Data: 10/04/2026 21:35:34.721 (UTC-0300)

Prof. Mestrando IAGO MORAIS DE OLIVEIRA MOURA
(AVALIADOR)

ZapSign d812f00e-9779-442d-9417-25e280de2228. Documento assinado eletronicamente, conforme MP 2.200-2/2001 e Lei 14.063/2020.

Dedico este trabalho à minha família, pelo apoio constante, pela compreensão e por sempre acreditarem na minha educação. A todos aqueles que, direta ou indiretamente, contribuíram para minha trajetória acadêmica, oferecendo incentivo, confiança e inspiração ao longo deste caminho.

“Privacidade não é sobre ter algo a esconder,
mas sobre ter o direito de controlar o que é
revelado sobre nós.”
Bruce Schneier

RESUMO

Este Trabalho de Conclusão de Curso (TCC) analisa os desafios jurídicos e de fiscalização enfrentados pela Autoridade Nacional de Proteção de Dados (ANPD) na aplicação do regime de Transferência Internacional de Dados Pessoais (TID), previsto no Artigo 33 da Lei Geral de Proteção de Dados (LGPD), especialmente quando confrontado com as operações de redes sociais estrangeiras. O problema central reside na tensão entre a Soberania Digital do Estado brasileiro e a Jurisdição Global das Big Techs, cujo modelo de negócio depende do fluxo transnacional de dados para perfilamento e publicidade. A pesquisa mapeou o arcabouço conceitual do direito fundamental à proteção de dados e sua manifestação na extraterritorialidade da LGPD (Art. 3º), que estabelece a soberania normativa brasileira. Utilizou-se metodologia qualitativa, de natureza dedutiva, com técnicas de pesquisa bibliográfica e documental, incluindo a análise das regulamentações da ANPD (Resolução CD/ANPD nº 19/2024) e a previsão de um estudo de caso. Argumenta-se que, embora o ordenamento jurídico brasileiro possua a base legal para impor a equivalência protetiva (Art. 33), a sua efetividade é gravemente limitada pelas barreiras jurisdicionais e pela assimetria de poder técnico e econômico entre a ANPD e os controladores globais. Conclui-se que o desafio não está na ausência de lei, mas sim na ausência de mecanismos eficazes de execução e sanção em face de agentes estrangeiros. O trabalho aponta, assim, para a necessidade urgente de fortalecimento da cooperação internacional e de redefinição do poder regulatório da ANPD para que o direito fundamental à proteção de dados seja efetivamente garantido aos titulares brasileiros.

Palavras-chave: soberania digital; transferência internacional de dados; fiscalização..

ABSTRACT

This monography paper analyzes the legal and enforcement challenges faced by the Brazilian National Data Protection Authority (ANPD) in the application of the regime of International Data Transfer (IDT), established in Article 33 of the Brazilian General Data Protection Law (LGPD), particularly when confronted with the operations of foreign social media platforms. The central issue lies in the tension between the Digital Sovereignty of the Brazilian State and the Global Jurisdiction of Big Tech companies, whose business model depends on the transnational flow of data for profiling and advertising. The research mapped the conceptual framework of the fundamental right to data protection and its manifestation in the extraterritoriality of the LGPD (Article 3), which establishes Brazilian normative sovereignty. A qualitative methodology of a deductive nature was adopted, using bibliographic and documentary research techniques, including the analysis of ANPD regulations (Resolution CD/ANPD No. 19/2024) and the development of a case study. It is argued that, although the Brazilian legal system provides the legal basis to impose protective equivalence (Article 33), its effectiveness is severely limited by jurisdictional barriers and by the asymmetry of technical and economic power between the ANPD and global data controllers. It is concluded that the challenge does not lie in the absence of legislation, but rather in the lack of effective mechanisms for enforcement and sanctions against foreign actors. The study therefore points to the urgent need to strengthen international cooperation and to redefine the regulatory power of the ANPD so that the fundamental right to data protection can be effectively guaranteed to Brazilian data subjects.

Key-words: digital sovereignty; international data transfer; enforcement.

LISTA DE ILUSTRAÇÕES

Figura 1 – Modelo esquemático do fluxo internacional de transferência de dados 28
Figura 2– Representação visual dos objetivos de pesquisa e suas respectivas análises 45

LISTA DE QUADROS

Quadro 1 – Comparação da incidência extraterritorial entre a LGPD e o GDPR 15

Quadro 2 – Estrutura da Transferência Internacional de Dados: LGPD (Pós-Res. 19/2024) vs. GDPR 23

Quadro 3 – Exigências da LGPD x declarações da META 33

LISTA DE ABREVIATURAS E SIGLAS

CF – CONSTITUIÇÃO FEDERAL

ANPD - Autoridade Nacional de Proteção de Dados.

CCJ - Centro de Ciências Jurídicas.

DPA - Data Protection Authority (Autoridade de Proteção de Dados).

GDPR - General Data Protection Regulation (Regulamento Geral sobre a Proteção de Dados da União Europeia).

LGPD - Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

MoU - Memorandum of Understanding (Memorando de Entendimento).

SCCs - Standard Contractual Clauses (Cláusulas Contratuais Padrão).

TCC - Trabalho de Conclusão de Curso.

TID - Transferência Internacional de Dados Pessoais.

UE - União Europeia.

UFPB - Universidade Federal da Paraíba

SUMÁRIO

1 INTRODUÇÃO **9**

2 A FUNDAMENTAÇÃO DA JURISDIÇÃO BRASILEIRA E O CONFLITO REGULATÓRIO NO CIBERESPAÇO **12**

2.1 A DELIMITAÇÃO DA SOBERANIA DIGITAL: DESAFIOS DO ESTADO NACIONAL NO AMBIENTE GLOBALIZADO 12

2.1.1 Do Território Físico ao Ciberespaço: Conceito de Soberania e Extraterritorialidade 12

2.1.2 O Princípio da Extraterritorialidade da LGPD (Art. 3º) como Instrumento de Tutela Jurídica Nacional 13

2.1.2.1 Análise Comparada da Extraterritorialidade (LGPD vs. GDPR) 14

2.1.3 A natureza do tratamento de dados nas redes sociais 18

2.2 A TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS (TID) COMO FOCO NO CONFLITO REGULATÓRIO 19

2.2.1 Fundamentos da TID e a Necessidade de Proteção Compatível com a LGPD 19

2.2.2 Análise Crítica dos Mecanismos de Transferência Regulamentados pela ANPD (Resolução CD/ANPD nº 19/2024) 20

2.3 LIMITES JURISDICIONAIS E AS BARREIRAS À EXECUÇÃO DA REGULAÇÃO BRASILEIRA 21

2.3.1 O Conflito de Jurisdição no Direito Internacional Privado Digital 21

2.3.2 Desafios de Fiscalização e Aplicação de Sanções (ANPD) a Controladores Internacionais 22

2.3.3 Cooperação Jurídica Internacional e Acordos Bilaterais como Vias de Superação da Barreira Jurisdicional 24

3 A EFETIVIDADE DO REGIME DE TRANSFERÊNCIA INTERNACIONAL DE DADOS E OS DESAFIOS DE CONFORMIDADE DAS PLATAFORMAS DIGITAIS **25**

3.1 O Artigo 33 da LGPD como Instrumento de Controle da Transferência Internacional 25

3.1.1 A Transferência Internacional de Dados e o Risco de Esvaziamento da Proteção Jurídica 27

3.2 O consentimento como base jurídica fragilizada na transferência internacional 29

3.3 Cláusulas contratuais padrão e decisão de adequação: entre a garantia formal e a eficácia operacional 30

3.4 A prática das plataformas digitais e a estrutura global da Meta 31

3.5 ESTUDO DE CASO: A TRANSFERÊNCIA INTERNACIONAL DE DADOS NA POLÍTICA DE PRIVACIDADE DA META 33

3.5.1 Delimitação metodológica do estudo 33

3.5.2 Identificação da Transferência Internacional 34

3.5.3 Bases jurídicas declaradas e enquadramento normativo 34

3.5.4 Transparência informacional e especificidade das transferências 35

3.5.5 Exercício de direitos e implicações jurisdicionais 36

3.5.6 Análise crítica à luz do artigo 33 da LGPD 36

4 OS LIMITES DA FISCALIZAÇÃO E OS DESAFIOS DA APLICAÇÃO E EXECUÇÃO DA LGPD NO CONTEXTO INTERNACIONAL **38**

4.1 Jurisdição normativa e jurisdição executiva no contexto da LGPD 38

4.2 Limitações na aplicação das sanções administrativas previstas na LGPD 38
4.3 Assimetria informacional e complexidade técnica na fiscalização das transferências internacionais 39
4.4 Cooperação internacional como condição para a efetividade da soberania digital 40
5 CONSIDERAÇÕES FINAIS 43

1 INTRODUÇÃO

Há muito tempo se diz que “internet é terra de ninguém”, e quanto mais plataformas surgem, mais descentralizada ela se torna. Em um ambiente global e desterritorializado, o desafio central reside em garantir que os direitos de privacidade e proteção de dados de cada usuário brasileiro não sejam violados (SARLET; CASSAROLI, 2022) . Essa preocupação se intensifica diante da atuação das grandes plataformas digitais, cujo modelo de negócio depende da coleta massiva, do perfilamento de usuários e da Transferência Internacional de Dados (TID) para fins econômicos, sobretudo publicidade comportamental. Vale ressaltar que, no presente trabalho, a expressão “modelo de negócios” refere-se ao modelo de plataformas digitais baseado em dados, descrito na literatura como capitalismo de plataforma (SRNICEK, *Platform Capitalism*, 2017). Trata-se de um modelo no qual as empresas geram valor por meio da coleta, do tratamento e da monetização de dados pessoais, sendo a Transferência Internacional de Dados elemento estrutural para o seu funcionamento, em razão da utilização de infraestruturas tecnológicas globalizadas. O termo não é utilizado no sentido de ferramentas gerenciais, como o Business Model Canvas.

A crise da soberania clássica, imposta pela intensa circulação transfronteiriça de tecnologia e dados (RANIERI, 2019) coloca em xeque a capacidade do Estado brasileiro de exercer sua soberania digital e proteger os direitos dos titulares.

Nesse contexto, a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) estabeleceu o princípio da extraterritorialidade (Art. 3º) e o regime de Transferência Internacional de Dados Pessoais (TID), notadamente em seu Artigo 33, regulamentado pela Resolução CD/ANPD nº 19/2024 (BRASIL, 2024). O princípio da extraterritorialidade permite que a lei brasileira seja aplicada a empresas estrangeiras quando suas atividades impactam indivíduos no Brasil. No caso da LGPD, isso garante a proteção de dados pessoais mesmo quando o tratamento ocorre fora do território nacional. A relevância desta pesquisa reside, portanto, em questionar se esses instrumentos são robustos o suficiente para resistir à jurisdição global das plataformas.

Nesse sentido, a problemática desta pesquisa está relacionada aos diversos desafios jurídicos e de fiscalização enfrentados pela Autoridade Nacional de Proteção de Dados (ANPD) para garantir o cumprimento dos requisitos previstos no artigo 33 da Lei Geral de Proteção de Dados, que disciplina a Transferência Internacional de Dados pessoais. A atuação de redes sociais estrangeiras que tratam dados de titulares brasileiros ocorre em ambiente transnacional, no qual os fluxos informacionais ultrapassam fronteiras estatais e dificultam a aplicação efetiva das normas nacionais de proteção de dados. Tal contexto evidencia tensões entre a soberania regulatória do Estado brasileiro e a jurisdição global das grandes plataformas digitais, cujas operações dependem da circulação internacional de dados.

A partir dessa problemática, levanta-se o seguinte problema central de pesquisa: os obstáculos enfrentados pela Autoridade Nacional de Proteção de Dados para garantir o cumprimento do regime de Transferência Internacional de Dados decorrem de uma insuficiência do arcabouço legislativo brasileiro ou da ausência de mecanismos eficazes de execução e aplicação das normas em face de agentes estrangeiros?

O objetivo primário para enfrentar essa problemática é analisar a efetividade da atuação da Autoridade Nacional de Proteção de Dados (ANPD) frente aos desafios impostos pela Transferência Internacional de Dados Pessoais (TID) realizada por redes sociais estrangeiras, no contexto da aplicação do artigo 33 da Lei Geral de Proteção de Dados Pessoais. Para alcançar esse objetivo geral, a pesquisa busca inicialmente mapear o conceito de Soberania Digital e examinar o alcance da extraterritorialidade da LGPD no contexto do modelo de negócios das redes sociais. Em seguida, pretende-se avaliar os mecanismos de garantia da Transferência Internacional de Dados previstos no artigo 33 da LGPD e em sua regulamentação infralegal, investigando sua adequação em relação aos Termos de Uso e às Políticas de Privacidade adotados pelas grandes plataformas digitais. Por fim, busca-se identificar os limites jurisdicionais e de fiscalização que dificultam a aplicação de sanções pela ANPD a agentes de tratamento de dados sediados no exterior.

O trabalho se justifica, então, pela sua relevância em três dimensões. Na dimensão jurídica e científica, a pesquisa é oportuna por se debruçar sobre o regime da Transferência Internacional de Dados, um dos pontos mais complexos da LGPD (DONEDA, [Ano]) e por analisar a recém-publicada regulamentação da ANPD. Essa análise qualifica o debate sobre a extraterritorialidade e a exigência de equivalência protetiva, em diálogo com o Direito Comparado (BIONI; MENDES, 2019). Na dimensão social e constitucional, o trabalho defende a efetivação do direito fundamental à proteção de dados pessoais, essencial para a autodeterminação informativa dos cidadãos. A crise da soberania clássica reforça a urgência de o Estado brasileiro exercer sua Soberania Digital (RANIERI, 2019) . Na dimensão regulatória, o estudo serve como subsídio crítico para avaliar a eficácia da intervenção estatal perante a assimetria de poder (MOREIRA NETO, 2014) .

Cumpre destacar, ainda, que o desenvolvimento desta pesquisa enfrenta o desafio de um tema recente, que carece de estudos e literatura, sobretudo nacional. A proteção de dados pessoais no Brasil constitui campo relativamente recente, especialmente após a entrada em vigor da LGPD e a consolidação institucional da Autoridade Nacional de Proteção de Dados. Em razão dessa recente evolução normativa e institucional, ainda há número limitado de doutrina consolidada, precedentes administrativos e estudos empíricos sobre a aplicação prática do regime de Transferência Internacional de Dados. Tal circunstância impõe desafios metodológicos, mas também reforça a relevância científica do estudo, ao contribuir para a construção inicial de reflexão acadêmica sobre a efetividade da soberania regulatória brasileira no ambiente digital.

Este trabalho está organizado em **cinco seções principais**, que serão desenvolvidas pela metodologia de pesquisa de natureza qualitativa, com abordagem exploratória e descritiva. As técnicas de pesquisa incluem a Pesquisa Bibliográfica, a Pesquisa Documental (com análise direta da LGPD, regulamentações e Termos de Uso de Big Techs), e o Estudo de Caso voltado à análise da Política de Privacidade da Meta Platforms, Inc., empresa responsável por plataformas amplamente utilizadas no Brasil, como Facebook e Instagram.

A investigação examinará as declarações institucionais da empresa acerca da transferência internacional de dados e confrontará tais práticas com os requisitos previstos no artigo 33 da LGPD e na regulamentação da ANPD, buscando identificar possíveis lacunas entre a conformidade formal declarada e a efetividade material das garantias de proteção de dados oferecidas aos titulares brasileiros.

Após esta Introdução (Capítulo 1), o desenvolvimento científico prossegue em três capítulos, utilizando o método de abordagem dedutivo, e partindo da análise da norma geral (LGPD) e da regulamentação específica (Resolução ANPD) para a verificação de sua aplicabilidade e efetividade no caso concreto das redes sociais estrangeiras. O Capítulo 2 mapeará o arcabouço conceitual e legal, discutindo a Soberania Digital e a aplicação da LGPD em âmbito internacional, cumprindo o primeiro objetivo específico. O Capítulo 3 avaliará em detalhe os requisitos da LGPD e os mecanismos regulamentares da ANPD, contrastando-os com as práticas de dados das Big Techs. O Capítulo 4 identificará as barreiras legais e práticas que impedem a fiscalização e a aplicação efetiva de sanções. Por fim, o Capítulo 5 (Considerações Finais) apresentará as conclusões correspondentes aos resultados da pesquisa, demonstrando se os objetivos foram alcançados.

2 A FUNDAMENTAÇÃO DA JURISDIÇÃO BRASILEIRA E O CONFLITO REGULATÓRIO NO CIBERESPAÇO

O presente capítulo tem como objetivo estabelecer o alicerce teórico-normativo que sustenta a capacidade regulatória brasileira sobre o tratamento de dados pessoais no âmbito transfronteiriço e, subsequentemente, detalhar como a movimentação de dados para o exterior se manifesta como o ponto focal do conflito jurisdicional. A análise inicia-se pela projeção da soberania do Estado no ciberespaço, avançando para o exame da extraterritorialidade da LGPD e, posteriormente culminando na avaliação da efetividade dos mecanismos de controle de Transferência Internacional de Dados (TID) implementados pela Autoridade Nacional de Proteção de Dados (ANPD).

2.1 A DELIMITAÇÃO DA SOBERANIA DIGITAL: DESAFIOS DO ESTADO NACIONAL NO AMBIENTE GLOBALIZADO

A natureza ubíqua e sem fronteiras da internet desafiou profundamente o paradigma tradicional do Direito, que historicamente ancorou sua eficácia na territorialidade física (SOARES, Pedro Silveira Campos. *Conflitos de leis de proteção de dados pessoais: Brasil e União Europeia em perspectiva*. 2023). A soberania estatal, entendida como o poder de um Estado impor sua lei e exercer seu poder de polícia em seu território, precisa ser repensada para lidar com a instantaneidade e a deslocalização do fluxo de dados.

2.1.1 Do Território Físico ao Ciberespaço: Conceito de Soberania e Extraterritorialidade

O surgimento da rede global de computadores deu origem ao debate sobre a governança, com a popularização da ideia de que a "internet é terra de ninguém". Vivemos em uma realidade onde a Big Tech assumiu a posição de soberana de dados de fato, desafiando a exclusividade da soberania tradicional dos Estados (GU, Hongfei. Data, Big Tech, and the New Concept of Sovereignty. Journal of Chinese Political Science).

Contudo, o impacto direto da atividade digital nos direitos fundamentais dos cidadãos tornou imprescindível a intervenção estatal. A impossibilidade de o Estado garantir direitos como a privacidade e a autodeterminação informativa no ciberespaço equivaleria a uma falha na tutela constitucional.

Neste contexto, a soberania digital é definida como a capacidade de um Estado de impor seus padrões normativos sobre os efeitos do tratamento de dados que incidem sobre seus cidadãos, independentemente da localização física do agente de tratamento ou do servidor onde o dado é armazenado. O Estado brasileiro, ao legislar sobre proteção de dados, exerce um imperativo constitucional de tutela, reconhecendo que a jurisdição deve se projetar para garantir direitos mesmo em ambientes não físicos.

2.1.2 O Princípio da Extraterritorialidade da LGPD (Art. 3º) como Instrumento de Tutela Jurídica Nacional

A Lei Geral de Proteção de Dados Pessoais (LGPD) formalizou a projeção da jurisdição brasileira ao estabelecer o princípio da extraterritorialidade em seu Artigo 3º. Esse dispositivo é o fundamento legal que permite ao Brasil regular a conduta de agentes de tratamento de dados (como as Big Techs) sediados no exterior.

> **Art. 3º** Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
>
> **I** – a operação de tratamento seja realizada no território nacional;
>
> **II** – a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
>
> **III** – os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
>
> **§ 1º** Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
>
> **§ 2º** Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

A lei brasileira incide sobre o tratamento de dados pessoais quando este é realizado no território nacional, quando dados são coletados no Brasil, ou, de forma mais crucial para a regulação das plataformas globais, quando a finalidade do tratamento é a oferta de bens ou serviços a indivíduos localizados no território nacional.

O Artigo 3º da LGPD estabelece o direito de regular (jurisdição prescritiva), afirmando a legitimidade legal do Estado brasileiro para pautar a conduta de empresas estrangeiras. No entanto, a mera existência da norma extraterritorial não é autossuficiente para garantir sua eficácia. A capacidade de punir e fiscalizar (jurisdição de execução) é um problema que transcende a legislação interna e depende de fatores externos, como a cooperação internacional. Isso indica que a base legal para a regulação está consolidada, mas a materialização dessa soberania digital ainda enfrenta obstáculos práticos complexos.

2.1.2.1 Análise Comparada da Extraterritorialidade (LGPD vs. GDPR)

A estrutura de incidência extraterritorial da LGPD demonstra uma clara inspiração e convergência com o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. O Artigo 3º da lei brasileira exibe uma alta similaridade com o Artigo 3º do GDPR. Ambos os arcabouços legais utilizam critérios baseados no alvo do tratamento (o titular) e no efeito econômico (oferta de serviços), permitindo que a lei nacional se aplique independentemente da sede física da empresa.

A Tabela 1 revela a aproximação normativa entre os dois regimes jurídicos. Ao confrontar os critérios de incidência territorial previstos na LGPD e no GDPR, observa-se que ambos adotam fundamentos semelhantes para justificar a aplicação extraterritorial de suas normas, especialmente quando o tratamento de dados envolve titulares localizados em seu território ou quando há oferta de bens e serviços direcionados a esses indivíduos.

Ideia-base da norma	LGPD	GDPR
Aplicação territorial da lei	**Art. 3º, I – LGPD**: aplica-se ao tratamento de dados realizado no território nacional.	**Art. 3º(1) – GDPR**: aplica-se ao tratamento de dados no contexto das atividades de estabelecimento de um controlador ou processador na União Europeia.
Aplicação extraterritorial baseada no titular	**Art. 3º, II – LGPD**: aplica-se ao tratamento de dados de indivíduos localizados no Brasil quando a atividade tem por objetivo a oferta ou fornecimento de bens ou serviços.	**Art. 3º(2)(a) – GDPR**: aplica-se quando bens ou serviços são oferecidos a titulares de dados localizados na União Europeia.
Aplicação extraterritorial baseada no monitoramento	**Art. 3º, II – LGPD**: inclui tratamento destinado ao monitoramento do comportamento de indivíduos localizados no Brasil.	**Art. 3º(2)(b) – GDPR**: aplica-se ao monitoramento do comportamento de titulares dentro da União Europeia.
Critério territorial da coleta	**Art. 3º, III – LGPD**: aplica-se quando os dados pessoais foram coletados no território nacional.	Não há previsão equivalente expressa no Art. 3º do GDPR.

Quadro 1: Comparação da incidência extraterritorial entre a LGPD e o GDPR (Elaboração própria com base no Art. 3º da Lei nº 13.709/2018 Lei Geral de Proteção de Dados Pessoais e no Art. 3º do Regulamento (UE) 2016/679 General Data Protection Regulation - GDPR).

A comparação também permite visualizar pequenas diferenças estruturais entre os dois modelos, como a previsão expressa, na LGPD, do critério territorial da coleta de dados, elemento que não aparece de forma equivalente no texto do GDPR. Assim, fica evidente que a legislação brasileira foi construída em diálogo com o modelo europeu, incorporando princípios semelhantes de proteção e **ampliando a capacidade do Estado** de aplicar sua legislação a empresas estrangeiras que tratam dados de seus cidadãos. (FINCK, Michèle. 2018)**.**

Essa convergência regulatória é vital para a credibilidade internacional da LGPD, pois sinaliza o alinhamento do Brasil com os **padrões globais de proteção de dados**. Adotar padrões semelhantes aos estabelecidos pelo GDPR é uma tática que pode reduzir o custo operacional e aumentar a **segurança jurídica** para as corporações multinacionais, facilitando sua adesão às regras brasileiras. Contudo, essa similaridade na jurisdição prescritiva não se traduz em equivalência nos mecanismos de execução, como evidenciam as diferenças nos tetos de multas e nos prazos de notificação.

2.1.2.2 A decisão de adequação no direito europeu e seus reflexos na soberania reguladora

No âmbito do Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a Transferência Internacional de Dados encontra disciplina no Capítulo V, especialmente nos artigos 44 a 49. Entre os mecanismos previstos, destaca-se a **Decisão de Adequação (Adequacy Decision)**, disciplinada no artigo 45 do GDPR. Trata-se de ato formal da Comissão Europeia que reconhece que determinado país ou organismo internacional oferece nível de proteção de dados essencialmente equivalente ao garantido pela legislação europeia.

Essa iniciativa se tornou essencial para a mudança do modelo americano, conforme analisam Houser e Voss (HOUSER, Kimberly A.; VOSS, W. Gregory. *Can Facebook and Google survive the GDPR?* Oxford Business Law Blog), a ideologia estadunidense prioriza o equilíbrio entre a capacidade das empresas de monetizar os dados coletados para incentivar a inovação e as expectativas de privacidade dos usuários, que tendem a ser consideravelmente menores nos Estados Unidos.

Contudo, no modelo europeu, quando um país é considerado adequado, as transferências de dados para seu território podem ocorrer sem necessidade de garantias adicionais, como cláusulas contratuais específicas, pois presume-se a equivalência regulatória. O processo de adequação envolve análise abrangente do ordenamento jurídico do país terceiro, incluindo: existência de legislação geral de proteção de dados; garantias de direitos fundamentais; mecanismos de fiscalização independentes; possibilidade de revisão judicial efetiva; compromissos internacionais assumidos.

Atualmente, o Brasil ainda **não possui decisão de adequação reconhecida pela União Europeia**, o que significa que transferências de dados da UE para o Brasil dependem de instrumentos adicionais, como cláusulas contratuais padrão. Sob a perspectiva da soberania regulatória, a decisão de adequação representa forma sofisticada de reconhecimento internacional da equivalência normativa.

Ao mesmo tempo, evidencia assimetria de poder regulatório, na medida em que **a União Europeia exerce posição central na definição de padrões globais de proteção de dados**. A ausência de reconhecimento de adequação pode impactar a competitividade internacional e reforça a necessidade de consolidação institucional da Autoridade Nacional de Proteção de Dados, cuja atuação eficaz é elemento relevante na avaliação de maturidade regulatória.

Assim, a decisão de adequação transcende aspecto meramente técnico, constituindo instrumento de projeção normativa e de afirmação de soberania digital no cenário internacional.

2.1.3 A natureza do tratamento de dados nas redes sociais

A compreensão da Transferência Internacional de Dados (TID) exige análise prévia da própria natureza do tratamento realizado pelas plataformas digitais. Redes sociais estruturam-se a partir de modelos econômicos baseados na coleta, análise e monetização de grandes volumes de dados pessoais, o que intensifica os desafios regulatórios examinados neste trabalho.

Diferentemente de modelos tradicionais de prestação de serviços, as plataformas digitais operam mediante **coleta massiva e contínua de dados**, abrangendo não apenas informações fornecidas diretamente pelo usuário (dados cadastrais, publicações, interações), mas também dados inferidos a partir de padrões comportamentais, geolocalização, preferências de consumo e histórico de navegação.

Esse ambiente favorece a prática do chamado **perfilamento (*profiling*)**, definido no artigo 5º, IV, da LGPD como forma de tratamento automatizado destinada a avaliar aspectos pessoais de uma pessoa natural, especialmente para analisar ou prever características relacionadas a desempenho profissional, interesses, comportamento ou localização. O perfilamento permite a construção de representações digitais detalhadas do usuário, que se tornam ativos econômicos relevantes no ecossistema digital. A partir dessas técnicas, desenvolve-se a chamada **publicidade comportamental**, modelo no qual anúncios são direcionados com base em perfis construídos algoritmicamente. Nesse contexto, os dados pessoais não são apenas meio de identificação, mas insumo central para segmentação mercadológica e maximização de receitas publicitárias. Tal dinâmica integra o fenômeno da ***data monetization***, pelo qual os dados passam a constituir recurso econômico estratégico. Ainda que as plataformas não “vendam” dados pessoais diretamente, sua exploração econômica ocorre por meio de segmentação publicitária, compartilhamento intragrupo e parcerias comerciais.

A configuração econômica e tecnológica das redes sociais demonstra que o fluxo internacional de dados não constitui elemento secundário ou meramente operacional, mas componente intrínseco ao seu funcionamento. A arquitetura descentralizada dessas plataformas, aliada à utilização de infraestruturas globais de armazenamento, processamento em nuvem e sistemas algorítmicos de análise comportamental, exige a circulação contínua de dados entre diferentes jurisdições. Nesse contexto, a Transferência Internacional de Dados não se apresenta como prática excepcional, mas como engrenagem estrutural da economia digital contemporânea, integrando o modelo de negócios das plataformas e condicionando sua própria viabilidade econômica.

2.2 A TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS (TID) COMO FOCO NO CONFLITO REGULATÓRIO

2.2.1 Fundamentos da TID e a Necessidade de Proteção Compatível com a LGPD

A Transferência Internacional de Dados (TID) constitui elemento estrutural do modelo de negócios das plataformas digitais globais, cujas infraestruturas distribuídas, sistemas de armazenamento em nuvem e mecanismos de publicidade comportamental dependem do fluxo contínuo de dados entre jurisdições. Contudo, quando dados pessoais são enviados a países que não oferecem grau de proteção equivalente ao da LGPD, surge tensão direta com o princípio da soberania digital, na medida em que o Estado brasileiro perde capacidade efetiva de controle sobre a tutela dos direitos fundamentais de seus titulares.

Não se trata de prática proibida pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). O artigo 33 admite a transferência, desde que observadas garantias específicas destinadas a assegurar nível de proteção compatível com o regime jurídico brasileiro. A TID é, portanto, juridicamente condicionada, e não livre. Para que a transferência seja autorizada, exige-se que o tratamento observe os princípios da finalidade, necessidade e transparência (art. 6º da LGPD), esteja amparado por base legal válida e se enquadre em um dos mecanismos previstos no próprio artigo 33, tais como decisões de adequação ou cláusulas contratuais padronizadas. O objetivo é impedir que a circulação internacional de dados funcione como mecanismo de evasão regulatória, assegurando que, mesmo fora do território nacional, os direitos dos titulares brasileiros permaneçam protegidos.

2.2.2 Análise Crítica dos Mecanismos de Transferência Regulamentados pela ANPD (Resolução CD/ANPD nº 19/2024)

Por um período, a ausência de regulamentação específica do Artigo 33 limitou a efetividade de diversos mecanismos previstos em lei.

A Autoridade Nacional de Proteção de Dados (ANPD) endereçou essa lacuna com a publicação da Resolução CD/ANPD nº 19/2024, em agosto de 2024, aprovando o Regulamento de Transferência Internacional de Dados Pessoais. Este regulamento representa a mais recente e concreta manifestação da intervenção estatal brasileira, aplicando a teoria da regulação ao controle da TID.

A Resolução 19/2024 detalhou os procedimentos para a Decisão de Adequação e estabeleceu o conteúdo das **Cláusulas Contratuais Padrão** (SCCs). A **Decisão de Adequação** é o instrumento pelo qual a ANPD **avalia** se um país estrangeiro ou organização internacional oferece um nível de proteção adequado de dados, considerando fatores que vão além da lei pura, abrangendo riscos, benefícios, impactos no fluxo de dados, e as relações diplomáticas, comércio e cooperação internacional.

Um aspecto de alta relevância é a regulamentação das SCCs, cujo período de graça para implementação foi concluído. As Cláusulas-Padrão Contratuais transformam a proteção de dados em uma obrigação contratual de direito privado com efeitos de direito público. Este mecanismo permite à ANPD fiscalizar e exigir garantias de proteção, mesmo quando o país de destino não possui uma Decisão de Adequação formal.

A Resolução exige que as cláusulas específicas sejam compatíveis com a LGPD e garantam um nível de proteção equivalente ao das SCCs nacionais. O alinhamento com a abordagem internacional (GDPR) visa promover a segurança jurídica para as empresas, ao mesmo tempo que mantém a autonomia regulatória brasileira.

Embora o Artigo 33 da LGPD preveja o **consentimento** do titular como uma das bases possíveis para a TID, a experiência e a doutrina especializada apontam para sua **fragilidade** operacional. A proteção de dados é balizada pelo princípio da autodeterminação informativa, que busca dar ao titular controle sobre seus dados. No contexto das redes sociais e do tratamento massivo de dados, as *Big Techs* frequentemente utilizam o consentimento obtido por meio de Termos de Uso genéricos e complexos para legitimar transferências internacionais volumosas.

O titular, ao aceitar o serviço, exerce formalmente sua vontade, mas, na prática, submete-se a condições predefinidas, limitando a eficácia da autodeterminação. A estratégia regulatória da ANPD, ao investir pesadamente em mecanismos institucionais e contratuais como as SCCs e a Decisão de Adequação, é um reconhecimento implícito de que o Consentimento (Art. 33, VIII) tende a ser a base legal mais vulnerável e menos robusta para lidar com a Transferência Internacional de Dados em larga escala.

2.3 LIMITES JURISDICIONAIS E AS BARREIRAS À EXECUÇÃO DA REGULAÇÃO BRASILEIRA

A plena efetividade da LGPD sobre agentes internacionais depende não apenas da existência da lei (jurisdição prescritiva), mas da capacidade da ANPD de impor penalidades e de fiscalizar o cumprimento (jurisdição de execução). Esta é a etapa em que a soberania digital enfrenta suas maiores barreiras.

2.3.1 O Conflito de Jurisdição no Direito Internacional Privado Digital

A extraterritorialidade permite que o Brasil legisle, mas o cumprimento de uma decisão judicial ou administrativa contra uma empresa sediada no exterior esbarra nas regras do Direito Internacional Privado sobre o foro e a execução. As *Big Techs* são, por natureza, deslocalizadas, o que dificulta a obtenção de provas, a citação formal e, principalmente, o processo de execução de multas.

Esse cenário pode ser observado, por exemplo, quando uma autoridade brasileira determina a aplicação de uma sanção administrativa ou judicial a uma empresa estrangeira que não possui sede ou ativos relevantes no Brasil.

Nesses casos, mesmo que a decisão seja válida no território nacional, sua execução prática pode depender de medidas adicionais, como o reconhecimento da decisão por autoridades estrangeiras ou a cooperação entre órgãos reguladores de diferentes países. Além disso, dados, servidores e documentos relevantes para a investigação podem estar armazenados em infraestruturas localizadas em outras jurisdições, o que dificulta a obtenção de provas e a efetiva fiscalização do tratamento de dados.

O conflito de jurisdição surge porque a imposição de uma sanção em um país depende da colaboração das autoridades do país onde o Controlador está sediado ou onde seus ativos estão localizados. A ausência de mecanismos claros de cooperação torna a aplicação da lei brasileira, nesse ponto, um desafio prático e legal complexo.

2.3.2 Desafios de Fiscalização e Aplicação de Sanções (ANPD) a Controladores Internacionais

A ANPD encontra severos limites jurisdicionais e de fiscalização ao tentar aplicar sanções a agentes de tratamento de dados sediados fora do país. Essa fragilidade é exacerbada pela disparidade no regime de penalidades do Brasil em comparação com o padrão global. (SOARES, Pedro Silveira Campos. 2023). Conforme será demonstrado no Quadro 2, enquanto o GDPR prevê multas que podem atingir o patamar de €20 milhões ou 4% do faturamento global (o que for maior), a LGPD impõe um teto máximo de R$ 50 milhões, limitado a 2% do faturamento da entidade no Brasil.

Critério	LGPD (Pós-Res. 19/2024)	GDPR (Arts. 44-50)
Decisão de Adequação	ANPD avalia nível de proteção, considerando relações diplomáticas e cooperação.	Comissão Europeia avalia.
Cláusulas Contratuais Padrão (SCCs)	Regulamentadas pela Resolução 19/2024; período de graça para implementação finalizado.	Amplamente estabelecidas e revisadas (SCCs da UE).
Teto Máximo de Multa	R$ 50 milhões (aproximadamente €11 milhões), 2% do faturamento no Brasil.	€ 20 milhões ou 4% do faturamento global (o que for maior).
Prazo para Reportar Incidentes	"Prazo razoável, conforme definido pela autoridade nacional" (aguardando definição estrita).	72 horas após a descoberta.

Quadro 2: Estrutura da Transferência Internacional de Dados: LGPD (Pós-Res. 19/2024) vs. GDPR (comparação entre as determinações da LGPD e da GDPR sobre transferência internacional de dados)

A combinação do teto de multa brasileiro significativamente mais baixo com a dificuldade operacional de execução transnacional resulta em uma capacidade de dissuasão (*deterrence*) limitada da ANPD sobre as gigantes globais. Para uma *Big Tech*, o risco de *compliance* associado à LGPD é menor do que o risco de não conformidade com outras jurisdições.

Consequentemente, a eficácia da jurisdição brasileira depende, em grande parte, da pressão regulatória exercida por outras autoridades de proteção de dados (DPAs) e da necessidade das empresas de manterem um padrão global de conformidade.

2.3.3 Cooperação Jurídica Internacional e Acordos Bilaterais como Vias de Superação da Barreira Jurisdicional

O principal caminho para superar o fosso entre o direito de regular e a capacidade de executar reside na cooperação jurídica internacional. A comunidade regulatória reconhece que a resolução de conflitos de jurisdição exige mecanismos de cooperação internacional que facilitem a aplicação das legislações nacionais.

A ANPD pode utilizar acordos de cooperação técnica e Memorandos de Entendimento (MoUs) com autoridades estrangeiras, como o já firmado com a Agência Espanhola de Proteção de Dados. Estes mecanismos facilitam o intercâmbio de informações e a coordenação de esforços de *enforcement*.

A colaboração com entidades de países como Estados Unidos, Reino Unido e Alemanha é crucial para transformar a fiscalização em um esforço multinacional. A dependência da cooperação projeta uma redefinição do conceito de soberania digital: para ser efetiva no ciberespaço, a soberania exige a delegação parcial de execução por meio de instrumentos de Direito Internacional Público e de uma intensa diplomacia reguladora.

Ao buscar essa convergência e assinar MoUs, a ANPD não apenas aumenta sua capacidade de *enforcement*, mas também fornece a segurança jurídica para as empresas, reduzindo a complexidade de operar em múltiplos regimes regulatórios. Em suma, a atuação eficaz do Brasil em relação à TID por empresas estrangeiras está intrinsecamente ligada à sua capacidade de integrar-se à governança global de dados.

3 A EFETIVIDADE DO REGIME DE TRANSFERÊNCIA INTERNACIONAL DE DADOS E OS DESAFIOS DE CONFORMIDADE DAS PLATAFORMAS DIGITAIS

O Capítulo anterior demonstrou que a soberania digital brasileira encontra fundamento jurídico na extraterritorialidade da LGPD (art. 3º) e que a Transferência Internacional de Dados (TID), disciplinada no art. 33, constitui o principal ponto de tensão entre a jurisdição estatal e a arquitetura global das plataformas digitais. Superada a etapa teórica, impõe-se agora examinar, em perspectiva crítica, se os mecanismos previstos no ordenamento brasileiro são efetivamente aptos a garantir a tutela dos direitos fundamentais dos titulares frente às práticas operacionais das Big Techs.

Este capítulo analisa, em primeiro lugar, os requisitos normativos do art. 33 da Lei nº 13.709/2018 e sua regulamentação pela Resolução CD/ANPD nº 19/2024; em seguida, confronta tais exigências com o modelo de tratamento de dados característico das plataformas digitais, marcado por coleta massiva, perfilamento e publicidade comportamental. O objetivo é avaliar se há compatibilidade estrutural entre o regime jurídico da TID e a lógica econômica que sustenta o ecossistema digital.

3.1 O Artigo 33 da LGPD como Instrumento de Controle da Transferência Internacional

A Transferência Internacional de Dados não é vedada pela Lei Geral de Proteção de Dados Pessoais. Ao contrário, o art. 33 admite expressamente sua realização, desde que observadas condições destinadas a assegurar nível de proteção compatível com o garantido no território nacional. Trata-se, portanto, de um regime de circulação condicionada, e não de proibição.

O dispositivo estabelece que a transferência somente poderá ocorrer nas hipóteses ali previstas, dentre as quais se destacam: (i) países ou organismos internacionais que proporcionem grau de proteção de dados adequado; (ii) garantias fornecidas pelo controlador por meio de cláusulas contratuais, normas corporativas globais ou selos e certificações; e (iii) hipóteses específicas, como consentimento do titular ou necessidade para execução de contrato.

Essa lógica dialoga diretamente com o modelo europeu previsto nos artigos 44 a 49 do GDPR, especialmente com o art. 45, que disciplina a decisão de adequação. Contudo, conforme já observado, o Brasil ainda não possui decisão de adequação reconhecida pela Comissão Europeia, o que revela assimetria regulatória no cenário internacional. No plano principiológico, o art. 33 deve ser interpretado em consonância com os fundamentos da LGPD, especialmente o respeito à privacidade, à autodeterminação informativa e à inviolabilidade da intimidade, dispostos nos artigos 1º e 2º da Lei nº 13.709/2018.

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Nesse sentido, a disciplina da Transferência Internacional de Dados não pode ser compreendida apenas como mecanismo técnico de circulação informacional, mas como instrumento destinado a impedir que o envio de dados ao exterior comprometa os direitos fundamentais que a própria lei busca proteger. Como destaca Danilo Doneda (2011), a proteção de dados integra o núcleo essencial dos direitos da personalidade na sociedade informacional, não se limitando ao controle formal do fluxo de informações.

Como destaca Danilo Doneda, a proteção de dados não se limita à disciplina formal do fluxo informacional, mas integra o núcleo essencial dos direitos da personalidade na sociedade informacional (DONEDA, 2011). Desse modo, a TID não pode funcionar como uma forma indireta de “escapar” da lei brasileira.

A transferência deve preservar, materialmente, o mesmo patamar de proteção assegurado internamente, sob pena de violação ao próprio fundamento constitucional do direito à proteção de dados, reconhecido expressamente no art. 5º, LXXIX, da Constituição Federal, incluído pela Emenda Constitucional nº 115/2022. Se a LGPD estabelece um conjunto de direitos e garantias no território nacional, esses mesmos padrões devem ser preservados quando os dados forem enviados ao exterior.

3.1.1 A Transferência Internacional de Dados e o Risco de Esvaziamento da Proteção Jurídica

Na prática, o risco surge quando empresas transferem dados pessoais para países que possuem legislação menos rigorosa ou mecanismos de fiscalização menos efetivos. Ainda que a empresa afirme cumprir formalmente a LGPD, pode ocorrer uma redução concreta do nível de proteção caso o ordenamento jurídico do país de destino não assegure direitos equivalentes aos previstos na lei brasileira. Nessa hipótese, a transferência funcionaria como um “atalho regulatório”, permitindo que dados de titulares brasileiros fiquem sujeitos a um regime mais frágil de tutela.

O artigo 33 da LGPD existe justamente para evitar esse cenário. Ao exigir decisão de adequação ou garantias contratuais específicas, o legislador buscou impedir que o simples deslocamento territorial dos dados resultasse em perda de proteção. A lógica do dispositivo é clara: a circulação internacional é permitida, mas não pode comprometer os direitos do titular.

Essa exigência ganha ainda mais relevância após a Emenda Constitucional nº 115/2022, que incluiu o direito à proteção de dados pessoais no artigo 5º, inciso LXXIX, da Constituição Federal. Ao reconhecer **a proteção de dados como direito fundamental**, a Constituição impõe que sua tutela seja preservada, **independentemente do local** onde o dado esteja **armazenado ou processado**. Assim, se a transferência internacional resultar, na prática, em diminuição das garantias asseguradas ao titular, poderá haver não apenas descumprimento da LGPD, mas também violação de direito fundamental.

Portanto, a análise da efetividade do regime de Transferência Internacional de Dados deve considerar não apenas a existência formal de cláusulas contratuais ou consentimentos genéricos, mas principalmente se o titular mantém, de maneira real e concreta, o mesmo nível de proteção que teria caso seus dados permanecessem sob jurisdição exclusivamente nacional. É nesse ponto que se revela o verdadeiro teste da soberania digital brasileira.



Ilustração 1 – modelo esquemático do fluxo de transferência internacional

3.2 O consentimento como base jurídica fragilizada na transferência internacional

Entre as hipóteses autorizadoras previstas no artigo 33 da LGPD, encontra-se o consentimento do titular (art. 33, VIII). Em tese, trata-se de manifestação legítima da autodeterminação informativa, fundamento expressamente reconhecido no art. 2º da Lei nº 13.709/2018.

Contudo, no contexto das redes sociais digitais e do tratamento massivo de dados, o consentimento revela fragilidades estruturais. As plataformas normalmente apresentam Termos de Uso e Políticas de Privacidade extensos, redigidos em linguagem técnica e com múltiplas finalidades agregadas. O usuário, ao aderir ao serviço, aceita integralmente as condições impostas, sem efetiva possibilidade de negociação.

Nessas circunstâncias, embora o consentimento seja formalmente obtido, questiona-se sua efetiva liberdade. Ingo Wolfgang Sarlet, ao examinar a dimensão objetiva e a eficácia dos direitos fundamentais, sustenta que sua proteção não se esgota na previsão normativa formal, exigindo condições reais para o exercício da liberdade pelo titular (SARLET, 2012). Aplicando essa construção ao contexto digital, se o titular não possui alternativa viável ao serviço ou não compreende adequadamente as consequências da transferência internacional, sua manifestação de vontade torna-se materialmente comprometida.

Além disso, a crítica à centralidade do consentimento encontra respaldo na doutrina de Danilo Doneda, que ao tratar da evolução do direito à proteção de dados destaca que a tutela não pode depender exclusivamente de escolhas individuais em ambientes marcados por forte assimetria informacional (DONEDA, 2011). O autor ressalta que o tratamento de dados na sociedade informacional ocorre em contextos estruturais de desequilíbrio entre titulares e agentes econômicos, o que limita a efetividade de soluções baseadas apenas na autonomia privada.

No mesmo sentido, Laura Schertel Mendes observa que a proteção de dados pessoais exige mecanismos estruturais de garantia, não sendo suficiente a simples obtenção formal do consentimento quando presentes situações de vulnerabilidade técnica e econômica do titular (MENDES, 2014).

3.3 Cláusulas contratuais padrão e decisão de adequação: entre a garantia formal e a eficácia operacional

Além do consentimento, o artigo 33 da Lei nº 13.709/2018 prevê mecanismos estruturais para legitimar a Transferência Internacional de Dados, especialmente a decisão de adequação e as garantias contratuais. Tais instrumentos foram regulamentados pela Resolução CD/ANPD nº 19/2024, que estabeleceu parâmetros objetivos para sua adoção.

A decisão de adequação, prevista no art. 33, I, da LGPD, permite que a Autoridade Nacional de Proteção de Dados reconheça que determinado país ou organismo internacional assegura nível de proteção compatível com o ordenamento brasileiro. Esse modelo guarda semelhança com o previsto no artigo 45 do Regulamento Geral de Proteção de Dados da União Europeia (GDPR), que atribui à Comissão Europeia a competência para declarar a adequação de países terceiros (UNIÃO EUROPEIA, Regulamento 2016/679, arts. 44-45).

No entanto, até o momento, o Brasil não possui decisão de adequação reconhecida pela União Europeia, o que demonstra que o reconhecimento internacional de equivalência normativa depende não apenas da existência formal da lei, mas da consolidação institucional de sua aplicação. Já as Cláusulas Contratuais Padrão (SCCs), regulamentadas pela Resolução CD/ANPD nº 19/2024, impõem obrigações específicas ao importador estrangeiro de dados, exigindo que este assegure direitos compatíveis com a LGPD. Trata-se de instrumento que transforma a proteção de dados em obrigação contratual vinculante.

Contudo, como observa Marçal Justen Filho ao tratar da regulação estatal, a eficácia de um modelo regulatório não depende apenas da norma posta, mas da capacidade de supervisão e imposição de consequências jurídicas em caso de descumprimento (JUSTEN FILHO, 2019).

No caso das SCCs, embora haja previsão formal de garantias, sua efetividade depende da possibilidade concreta de fiscalização e aplicação de sanções pela ANPD.

Além disso, o titular dos dados raramente possui acesso direto às cláusulas firmadas entre controlador e operador estrangeiro, o que limita a transparência e o controle social sobre o cumprimento das obrigações assumidas. Assim, o instrumento contratual, embora juridicamente robusto, pode revelar fragilidades quando confrontado com estruturas empresariais globalizadas e descentralizadas.

3.4 A prática das plataformas digitais e a estrutura global da Meta

A Meta Platforms, Inc., controladora do Facebook e do Instagram, constitui exemplo paradigmático de empresa que opera sob arquitetura globalizada de dados.

Segundo a Política de Privacidade da Meta, atualizada em 2023, a empresa informa que os dados dos usuários podem ser transferidos e processados nos Estados Unidos e em outros países onde suas afiliadas ou prestadores de serviço estejam localizados (META PLATFORMS, INC., *Privacy Policy*, 2023).

A política declara que essas transferências podem ocorrer com fundamento em mecanismos jurídicos como Cláusulas Contratuais Padrão e outros instrumentos previstos nas legislações aplicáveis. Do ponto de vista da Lei nº 13.709/2018, tais operações configuram hipótese de Transferência Internacional de Dados, nos termos do art. 5º, inciso XV, e devem observar as condições estabelecidas no art. 33 da mesma lei. A política afirma que tais transferências são realizadas com base em:

- Cláusulas Contratuais Padrão aprovadas pela Comissão Europeia;
- decisões de adequação quando aplicáveis;
- outros mecanismos legais previstos na legislação aplicável.

Do ponto de vista jurídico brasileiro, tais transferências configuram hipótese de Transferência Internacional de Dados nos termos do art. 5º, XV, da Lei nº 13.709/2018. A seguir, apresenta-se quadro comparativo entre exigências normativas da LGPD e práticas declaradas pela Meta:

Critério	Exigência Legal (LGPD)	Prática Declarada pela Meta
Base legal para TID	Art. 33, I e IX – transferência internacional permitida mediante adequação do país de destino ou consentimento específico do titular	Consentimento + SCCs + mecanismos internacionais
Transparência	Art. 9º – obrigação de fornecer informações claras e acessíveis sobre o tratamento de dados	Informação genérica sobre transferências globais
País de destino	Art. 33 – necessidade de garantia de nível adequado de proteção de dados no país receptor	Indicação ampla do destino dos dados: “EUA e outros países”
Garantias	Cláusulas padrão (Res. 19/2024) - utilização de cláusulas contratuais ou mecanismos que assegurem proteção equivalente à LGPD	Uso de SCCs europeias
Exercício de direitos	Arts. 18 e 33 - garantia de acesso, correção, eliminação e demais direitos do titular	Ferramentas digitais da própria plataforma para acesso, download, correção ou exclusão de dados

Quadro 3 – exigências da LGPD X declarações da META (Fonte: Lei nº 13.709/2018; Resolução CD/ANPD nº 19/2024; META, Privacy Policy)

A análise comparativa apresentada na tabela evidencia que a política de privacidade da Meta procura demonstrar aderência formal aos requisitos previstos na legislação de proteção de dados.

A empresa declara utilizar mecanismos jurídicos reconhecidos internacionalmente para legitimar as transferências de dados, como cláusulas contratuais padrão, além de disponibilizar ferramentas digitais para que os usuários possam exercer seus direitos previstos na legislação.

Na prática, esses direitos são operacionalizados por meio de funcionalidades disponibilizadas dentro das próprias plataformas, como ferramentas para acesso, download, correção ou exclusão de dados pessoais. Esse modelo revela que o exercício dos direitos do titular ocorre dentro da própria infraestrutura tecnológica da empresa, o que significa que o processo permanece sob controle da plataforma.

Como consequência, a autoridade reguladora passa a depender, em grande medida, das informações fornecidas pela própria empresa para verificar a conformidade do tratamento de dados. Essa dinâmica evidencia uma assimetria estrutural de poder entre a Autoridade Nacional de Proteção de Dados e as grandes plataformas digitais, aspecto que reforça os desafios práticos de fiscalização e aplicação efetiva das normas de proteção de dados no contexto das transferências internacionais.

3.5 ESTUDO DE CASO: A TRANSFERÊNCIA INTERNACIONAL DE DADOS NA POLÍTICA DE PRIVACIDADE DA META

3.5.1 Delimitação metodológica do estudo

O presente estudo de caso consiste em análise documental da Política de Privacidade da Meta Platforms, Inc., atualizada em 2023, aplicável às plataformas Facebook e Instagram (META PLATFORMS, INC., *Privacy Policy*, 2023). A escolha da empresa justifica-se por sua atuação massiva no Brasil, pela natureza globalizada de sua infraestrutura tecnológica e pela expressa previsão de transferência internacional de dados em sua política pública de privacidade. O objetivo da análise é verificar a conformidade das práticas declaradas pela empresa com os requisitos estabelecidos no artigo 33 da Lei nº 13.709/2018 (LGPD), bem como com a regulamentação introduzida pela Resolução CD/ANPD nº 19/2024.

3.5.2 Identificação da Transferência Internacional

A Política de Privacidade da Meta informa que os dados podem ser transferidos e processados nos Estados Unidos e em outros países onde a empresa possua afiliadas, parceiros ou prestadores de serviço (META PLATFORMS, INC., 2023).

Nos termos do artigo 5º, inciso XV, da Lei nº 13.709/2018, considera-se Transferência Internacional de Dados qualquer transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro. Assim, as operações descritas pela Meta enquadram-se formalmente no conceito legal de Transferência Internacional de Dados. Importa observar que a política não apresenta a transferência como evento excepcional, mas como elemento estrutural do funcionamento da plataforma, o que indica que o fluxo internacional integra o próprio modelo operacional da empresa.

Importa destacar que, no caso analisado, a transferência não é eventual ou acessória, mas integra o próprio funcionamento técnico da plataforma. A arquitetura digital da empresa, baseada em centros de dados distribuídos e processamento transnacional, indica que a circulação internacional é componente estrutural do modelo econômico adotado. Isso significa que o regime do artigo 33 da LGPD incide não sobre situação excepcional, mas sobre prática cotidiana e sistemática.

3.5.3 Bases jurídicas declaradas e enquadramento normativo

A Política de Privacidade da Meta declara que as transferências internacionais são realizadas com fundamento em diferentes bases jurídicas, a depender da operação envolvida. Entre as justificativas apresentadas estão a execução de contrato, o legítimo interesse empresarial, o consentimento do titular quando exigido pela legislação aplicável e a utilização de Cláusulas Contratuais Padrão como mecanismo de garantia.

No ordenamento brasileiro, entretanto, a legitimidade da transferência internacional não depende apenas da existência de base legal para o tratamento, nos termos do artigo 7º da LGPD. É necessário também o enquadramento em uma das hipóteses específicas previstas no artigo 33 da Lei nº 13.709/2018.

A mera invocação de execução contratual ou legítimo interesse não substitui a necessidade de observância dos mecanismos próprios de transferência internacional.

A política da Meta menciona a adoção de Cláusulas Contratuais Padrão como salvaguarda jurídica para transferências destinadas a países que não possuam decisão de adequação. Esse modelo encontra paralelo no artigo 46 do Regulamento (UE) 2016/679 (GDPR) e foi regulamentado no Brasil pela Resolução CD/ANPD nº 19/2024. Contudo, na versão pública da política analisada, não há detalhamento sobre a adaptação dessas cláusulas ao regime brasileiro, tampouco disponibilização do conteúdo contratual específico aplicável aos titulares situados no Brasil.

Assim, observa-se conformidade formal quanto à indicação de mecanismo reconhecido internacionalmente, mas permanece limitada a possibilidade de verificação material da equivalência de proteção exigida pelo artigo 33 da LGPD.

3.5.4 Transparência informacional e especificidade das transferências

O artigo 9º da Lei nº 13.709/2018 determina que o titular deve receber informações claras, adequadas e ostensivas acerca do tratamento de seus dados pessoais. A Política de Privacidade da Meta informa que os dados podem ser transferidos para os Estados Unidos e para “outros países” onde a empresa atue ou mantenha parceiros comerciais.

Embora essa informação indique a existência de transferência internacional, sua formulação genérica limita a compreensão concreta do titular quanto aos destinos específicos de seus dados. Não há, na versão analisada, lista detalhada de países envolvidos, nem discriminação individualizada das operações realizadas em cada jurisdição.

Essa generalidade cumpre formalmente o dever de informar, mas pode comprometer a transparência material exigida pela LGPD. O titular, ao não saber com precisão onde seus dados serão processados, encontra dificuldades para avaliar o nível de proteção aplicável ou para identificar autoridades reguladoras competentes em caso de violação.

3.5.5 Exercício de direitos e implicações jurisdicionais

A Meta disponibiliza mecanismos digitais para o exercício dos direitos previstos na legislação de proteção de dados, incluindo acesso, correção e exclusão de informações, em consonância com o artigo 18 da LGPD. Contudo, quando o processamento ocorre em múltiplas jurisdições, o exercício efetivo desses direitos pode depender da articulação entre diferentes unidades corporativas e sistemas jurídicos.

O artigo 3º da Lei nº 13.709/2018 estabelece a aplicação extraterritorial da LGPD sempre que o tratamento de dados tiver como objetivo a oferta de bens ou serviços a indivíduos localizados no Brasil. Entretanto, a capacidade concreta de fiscalização e execução de sanções contra empresa sediada no exterior pode depender de mecanismos de cooperação internacional.

Desse modo, o caso evidencia a distinção entre jurisdição normativa, que permite ao Estado brasileiro regular a atividade, e jurisdição executiva, que condiciona a efetividade prática dessa regulação.

3.5.6 Análise crítica à luz do artigo 33 da LGPD

A análise da Política de Privacidade da Meta permite concluir que há reconhecimento expresso da transferência internacional e indicação de mecanismos jurídicos destinados a legitimar a operação. Sob a perspectiva formal, a empresa demonstra preocupação em alinhar suas práticas aos padrões internacionais de proteção de dados.

Todavia, sob a perspectiva material, persistem questionamentos quanto à efetiva equivalência de proteção assegurada ao titular brasileiro. A indicação genérica de países de destino, a ausência de detalhamento público das cláusulas contratuais e a dependência de estruturas transnacionais de fiscalização evidenciam que a conformidade normativa não elimina os desafios práticos da proteção de dados em ambiente globalizado.

O estudo de caso revela, portanto, que a Transferência Internacional de Dados realizada pela Meta apresenta aderência formal ao modelo previsto no artigo 33 da LGPD e na Resolução CD/ANPD nº 19/2024, mas sua efetividade concreta depende da capacidade institucional da ANPD de fiscalizar tais mecanismos e da existência de cooperação internacional eficaz.

Essa constatação prepara o exame, no capítulo seguinte, das barreiras estruturais que limitam o reforço da soberania digital brasileira diante de conglomerados tecnológicos de atuação global.

4 OS LIMITES DA FISCALIZAÇÃO E OS DESAFIOS DA APLICAÇÃO E EXECUÇÃO DA LGPD NO CONTEXTO INTERNACIONAL

4.1 Jurisdição normativa e jurisdição executiva no contexto da LGPD

O estudo de caso analisado no capítulo anterior evidenciou que grandes plataformas digitais, como a Meta Platforms, Inc., adotam mecanismos formais para legitimar a Transferência Internacional de Dados. Entretanto, a conformidade declarada não elimina a necessidade de examinar a efetividade prática do regime jurídico brasileiro.

A Lei nº 13.709/2018 estabelece, em seu artigo 3º, a aplicação extraterritorial da LGPD sempre que o tratamento de dados tiver por objetivo a oferta de bens ou serviços a indivíduos localizados no Brasil ou quando os dados forem coletados em território nacional. Tal dispositivo representa uma afirmação expressa da jurisdição normativa brasileira no ambiente digital.

Contudo, a competência para legislar (jurisdição prescritiva) não se confunde com a capacidade de impor, na prática, o cumprimento das obrigações (jurisdição executiva). No plano do Direito Internacional, a execução de medidas coercitivas contra empresa sediada no exterior, pode depender de mecanismos de cooperação jurídica internacional e reconhecimento mútuo de decisões administrativas.

Como observa Ranieri, a soberania no contexto globalizado não se exerce de forma isolada, mas dentro de um sistema de interdependência entre ordens jurídicas (RANIERI, Teoria do Estado e da Constituição, 2019). Assim, embora o Brasil tenha afirmado sua autoridade regulatória sobre o tratamento de dados de seus cidadãos, a concretização dessa autoridade enfrenta limites estruturais quando o agente econômico está sediado fora do território nacional.

4.2 Limitações na aplicação das sanções administrativas previstas na LGPD

A efetividade do regime de Transferência Internacional de Dados não depende apenas da afirmação da extraterritorialidade da lei, mas também da possibilidade concreta de responsabilização em caso de descumprimento.

Nesse sentido, o artigo 52 da Lei nº 13.709/2018 prevê sanções administrativas que incluem advertência, multa simples, multa diária, publicização da infração, bloqueio e eliminação de dados pessoais.

A multa simples pode alcançar até dois por cento do faturamento da pessoa jurídica no Brasil, limitada ao valor máximo de cinquenta milhões de reais por infração. Quando se analisa esse limite à luz da dimensão econômica de conglomerados tecnológicos globais, como demonstrado no estudo de caso da Meta, surge questionamento quanto ao seu potencial dissuasório.

Danilo Bioni sustenta que a regulação da economia de dados deve ser capaz de alterar os incentivos econômicos dos agentes de tratamento, sob pena de se tornar meramente declaratória ou simbólica (BIONI, Proteção de Dados Pessoais: A Função e os Limites do Consentimento, 2019). Se a sanção não representa impacto econômico relevante para a empresa, a tendência é que seja internalizada como custo operacional, e não como elemento de transformação estrutural de condutas.

Em comparação, o Regulamento (UE) 2016/679, em seu artigo 83, prevê multas que podem atingir até quatro por cento do faturamento global anual da empresa. A diferença entre faturamento nacional e faturamento global evidencia disparidade significativa na capacidade de pressão econômica do regime sancionatório.

Além da limitação quantitativa, há a questão da execução internacional das sanções. Caso a empresa possua sede e ativos majoritariamente localizados no exterior, a cobrança coercitiva de multa poderá depender de mecanismos de cooperação jurídica internacional. A ausência de instrumentos eficazes de execução pode reduzir a força prática da norma, ainda que sua validade jurídica permaneça intacta.

4.3 Assimetria informacional e complexidade técnica na fiscalização das transferências internacionais

O estudo de caso da Meta revelou que a Transferência Internacional de Dados ocorre dentro de infraestrutura técnica globalizada, envolvendo múltiplos centros de processamento, contratos transnacionais e cadeias de sub-operadores. Essa estrutura amplia a complexidade da fiscalização regulatória.

Danilo Doneda afirma que a proteção de dados pessoais, na sociedade informacional, exige mecanismos institucionais capazes de enfrentar estruturas complexas de tratamento automatizado, sob pena de a tutela jurídica tornar-se meramente formal (DONEDA, 2011). No contexto das transferências internacionais, essa advertência ganha especial relevância.

A assimetria informacional, conceito desenvolvido por Danilo Bioni ao examinar a economia de dados, manifesta-se não apenas na relação entre titular e empresa, mas também entre regulador e regulado (BIONI, 2019). Grandes plataformas detêm conhecimento técnico aprofundado sobre suas arquiteturas de dados, enquanto a autoridade reguladora depende de informações fornecidas pela própria empresa para avaliar a conformidade.

Laura Schertel Mendes destaca que a proteção de dados demanda instrumentos estruturais de responsabilização que transcendam a mera formalidade contratual (MENDES, 2014). A simples existência de cláusulas contratuais padrão, mencionadas na política de privacidade da Meta, não assegura, por si só, que a equivalência material de proteção exigida pelo artigo 33 da LGPD esteja sendo efetivamente observada.

A fiscalização de fluxos internacionais exige capacidade técnica especializada, inclusive para análise de arquitetura de servidores, fluxos transfronteiriços e mecanismos de segurança. Assim, a consolidação institucional e técnica da Autoridade Nacional de Proteção de Dados constitui elemento central para a efetividade do regime jurídico brasileiro.

4.4 Cooperação internacional como condição para a efetividade da soberania digital

A própria Lei nº 13.709/2018 reconhece a dimensão internacional da proteção de dados ao atribuir à ANPD competência para promover cooperação com autoridades estrangeiras, conforme previsto no artigo 55-J, inciso XIII.

Em contexto de circulação global de dados, a soberania não se exerce de maneira isolada, mas por meio de articulação entre ordens jurídicas. A interdependência regulatória torna-se condição estrutural para a proteção efetiva dos titulares.

Danilo Doneda sustenta que a proteção de dados constitui instrumento de tutela da personalidade na sociedade informacional e depende de estruturas

institucionais aptas a assegurar sua aplicação concreta (DONEDA, 2011). Em ambiente transnacional, essa estrutura necessariamente envolve mecanismos de cooperação internacional.

> "Enquanto a soberania tradicional se baseia em fronteiras físicas, a infosfera exige uma gestão do pluralismo jurídico. Nesse cenário, as Big Techs emergem como novos 'Leviatãs' digitais, exercendo um poder de fato sobre os dados que muitas vezes supera a capacidade de fiscalização dos Estados. A fiscalização pela ANPD no Brasil enfrenta, portanto, o desafio de notificar agentes que, embora atuem no mercado nacional, não possuem sede física, utilizando-se da ubiquidade dos dados para operar em um espaço desterritorializado." (**SOARES, Pedro Silveira Campos**. 2023)

A consolidação de acordos de cooperação técnica, intercâmbio de informações e articulação com outras autoridades de proteção de dados pode ampliar a capacidade de fiscalização da ANPD, especialmente em casos envolvendo empresas sediadas fora do Brasil. Sem essa coordenação, a aplicação extraterritorial da LGPD tende a encontrar barreiras práticas. A análise desenvolvida ao longo deste capítulo, em diálogo direto com o estudo de caso da Meta apresentado anteriormente, demonstra que o Brasil dispõe de base normativa consistente para disciplinar a Transferência Internacional de Dados, especialmente por meio do artigo 3º e do artigo 33 da Lei nº 13.709/2018, bem como da Resolução CD/ANPD nº 19/2024.

Entretanto, a efetividade desse regime encontra limites estruturais relacionados à execução internacional de sanções, à limitação econômica das multas administrativas, à assimetria técnica entre regulador e plataformas digitais e à necessidade de cooperação internacional para fiscalização transnacional.A soberania digital brasileira, portanto, revela-se como construção normativa relevante, cuja consolidação prática depende do fortalecimento institucional da ANPD e da inserção estratégica do Brasil em redes internacionais de proteção de dados.

Essas conclusões preparam o exame final a ser desenvolvido no Capítulo 5, no qual será avaliado, de forma crítica e sistematizada, se o regime jurídico brasileiro de Transferência Internacional de Dados é suficiente para assegurar proteção efetiva aos titulares ou se demanda aperfeiçoamentos estruturais e institucionais.

5 CONSIDERAÇÕES FINAIS

O presente trabalho teve como objetivo analisar a efetividade do regime jurídico brasileiro de Transferência Internacional de Dados, com especial atenção ao artigo 33 da Lei nº 13.709/2018 e aos mecanismos regulamentares instituídos pela Autoridade Nacional de Proteção de Dados, avaliando sua aplicação prática no contexto das plataformas digitais estrangeiras.

A pesquisa foi orientada pelo seguinte problema central: os obstáculos enfrentados pela Autoridade Nacional de Proteção de Dados para garantir o cumprimento do regime de Transferência Internacional de Dados decorrem de uma insuficiência do arcabouço legislativo brasileiro ou da ausência de mecanismos eficazes de execução e aplicação das normas em face de agentes estrangeiros?

Essa questão parte da constatação de que, embora o ordenamento jurídico nacional tenha desenvolvido instrumentos normativos para regular o fluxo internacional de dados, a atuação de empresas transnacionais que operam em ambiente digital globalizado desafia os mecanismos tradicionais de fiscalização e aplicação do direito.

A pesquisa demonstrou, inicialmente, que a proteção de dados pessoais foi elevada ao patamar de direito fundamental pela Emenda Constitucional nº 115/2022, que incluiu o artigo 5º, inciso LXXIX, na Constituição Federal. Esse reconhecimento reforça a centralidade da tutela da informação pessoal no ordenamento jurídico brasileiro e impõe ao Estado o dever de estruturar mecanismos eficazes de proteção, inclusive no contexto internacional.

No plano infraconstitucional, a Lei nº 13.709/2018 estabeleceu regime detalhado para a Transferência Internacional de Dados, especialmente por meio do artigo 33, que condiciona a circulação transfronteiriça à observância de hipóteses específicas e garantias adequadas. A regulamentação posterior promovida pela Resolução CD/ANPD nº 19/2024 contribuiu para conferir maior densidade normativa ao sistema, disciplinando critérios de adequação e cláusulas contratuais padrão.

Do ponto de vista normativo, portanto, o Brasil dispõe de arcabouço jurídico alinhado a padrões internacionais, aproximando-se do modelo europeu previsto no Regulamento (UE) 2016/679.

A previsão de extraterritorialidade no artigo 3º da LGPD, bem como a existência de sanções administrativas no artigo 52, evidenciam a intenção de afirmar a soberania regulatória brasileira no ambiente digital.

Entretanto, a análise prática desenvolvida por meio do estudo de caso da Meta Platforms, Inc. revelou que a conformidade formal com os mecanismos previstos na legislação não elimina desafios estruturais relacionados à transparência, fiscalização e execução de sanções.

A utilização de cláusulas contratuais padrão e a menção genérica a transferências globais atendem, em tese, aos requisitos formais da lei, mas a verificação material da equivalência de proteção depende da capacidade institucional da Autoridade Nacional de Proteção de Dados.

Além disso, a limitação do valor das multas ao faturamento obtido no Brasil, prevista no artigo 52 da LGPD, pode reduzir o potencial dissuasório do regime sancionatório quando aplicado a conglomerados multinacionais. A execução internacional de sanções, por sua vez, pode demandar cooperação jurídica entre Estados, evidenciando que a efetividade da norma não depende apenas da sua redação, mas da articulação institucional entre autoridades reguladoras.

Diante desse conjunto de elementos, os resultados da pesquisa indicam que o principal desafio enfrentado pelo regime brasileiro de Transferência Internacional de Dados não reside na ausência de normas jurídicas, mas nas dificuldades práticas de fiscalização e execução dessas normas no contexto transnacional em que operam as grandes plataformas digitais. A legislação brasileira estabelece parâmetros relevantes de proteção e se encontra alinhada a padrões internacionais, porém sua efetividade depende de mecanismos institucionais capazes de enfrentar a natureza global da economia digital.

Dessa forma, a hipótese implícita que orientou a pesquisa foi confirmada: o ordenamento jurídico brasileiro possui estrutura normativa adequada para disciplinar a Transferência Internacional de Dados, mas sua aplicação concreta enfrenta limites estruturais decorrentes da dificuldade de execução de sanções contra agentes estrangeiros, da dependência de cooperação jurídica internacional e da assimetria técnica e informacional existente entre autoridades reguladoras e grandes empresas de tecnologia.



Ilustração 2 - representação visual dos objetivos de pesquisa e suas respectivas análises

Conclui-se, portanto, que a soberania digital brasileira não está ausente no plano normativo, uma vez que o país já dispõe de legislação específica para regular a Transferência Internacional de Dados, especialmente por meio da Lei Geral de Proteção de Dados.

No entanto, a efetividade dessa regulação ainda depende do fortalecimento institucional da Autoridade Nacional de Proteção de Dados, do desenvolvimento de mecanismos de cooperação internacional entre autoridades reguladoras e da criação de instrumentos mais eficazes de fiscalização e execução de sanções. Esses elementos são fundamentais para garantir que a transferência de dados para o exterior não comprometa a proteção dos direitos fundamentais dos titulares brasileiros.

Assim, os objetivos propostos no início da pesquisa foram alcançados. O estudo permitiu, em primeiro lugar, examinar o conceito de soberania digital e o alcance da extraterritorialidade da Lei Geral de Proteção de Dados no contexto das plataformas digitais globais.

Em seguida, foi possível analisar os mecanismos jurídicos que regulam a Transferência Internacional de Dados previstos no artigo 33 da LGPD e em sua regulamentação, confrontando tais exigências com as práticas declaradas por empresas do setor tecnológico.

Por fim, a pesquisa identificou os principais limites jurisdicionais e institucionais que dificultam a atuação fiscalizatória da Autoridade Nacional de Proteção de Dados diante de empresas sediadas no exterior.

A pesquisa contribui, portanto, para o debate sobre proteção de dados e soberania digital ao demonstrar que a garantia desse direito fundamental não depende apenas da existência de normas jurídicas, mas também da capacidade do Estado de aplicá-las de forma efetiva em um ambiente digital marcado pela atuação global das grandes empresas de tecnologia.

REFERÊNCIAS

BEIRIZ, Bernardo; LANNES, Daniel; NICHELLI, Juliane; MENDES, Maria Clara; FERREIRA, Nathan. *Regulação das Big Techs: o que dizem os atores envolvidos?* Rio de Janeiro: Instituto de Relações Internacionais (IRI), 2021

BIONI, Danilo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2019.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, 1988.

BRASIL. Autoridade Nacional de Proteção de Dados. *Resolução CD/ANPD nº 19, de 23 de agosto de 2024*. Dispõe sobre a Transferência Internacional de Dados Pessoais. Brasília, DF: ANPD, 2024.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Brasília, DF: Presidência da República, 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Brasília, DF: Presidência da República, 2018.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709/2018 e dispõe sobre a criação da Autoridade Nacional de Proteção de Dados (ANPD). Brasília, DF: Presidência da República, 2019.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados*. Rio de Janeiro: Renovar, 2011.

FINCK, Michèle. Google v CNIL: *Defining the Territorial Scope of European Data Protection Law*. Oxford Business Law Blog (OBLB), 16 de novembro de 2018

GU, Hongfei. *Data, Big Tech, and the New Concept of Sovereignty*. Journal of Chinese Political Science, publicado online em 3 de maio de 2023. Disponível em: https://doi.org/10.1007/s11366-023-09855-1

HOUSER, Kimberly A.; VOSS, W. Gregory. *Can Facebook and Google survive the GDPR?* Oxford Business Law Blog (OBLB), 29 de agosto de 2018

SOARES, Pedro Silveira Campos. *Conflitos de leis de proteção de dados pessoais: Brasil e União Europeia em perspectiva*. 2023. 139 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade Federal de Minas Gerais, Belo Horizonte, 2023

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. São Paulo: Revista dos Tribunais, 2014.

META PLATFORMS, INC. *Privacy Policy*. Menlo Park, 2023.

RANIERI, Nina Beatriz Stocco. *Teoria do Estado e da Constituição*. 3. ed. Barueri: Manole, 2019.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Caso C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd e Maximillian Schrems (Schrems II)*. Luxemburgo, 16 jul. 2020.

UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016*. Regulamento Geral sobre a Proteção de Dados (GDPR). Jornal Oficial da União Europeia, Bruxelas, 2016.

APÊNDICE A – NOME DO APÊNDICE

APÊNDICE A – PROCEDIMENTO METODOLÓGICO DA ANÁLISE DOCUMENTAL

A análise do estudo de caso foi realizada por meio de pesquisa documental qualitativa, tendo como objeto a Política de Privacidade da Meta Platforms, Inc., versão 2023. O procedimento consistiu na leitura integral do documento, identificação de trechos relacionados à Transferência Internacional de Dados e posterior confrontação com os requisitos previstos no artigo 33 da Lei nº 13.709/2018 e na Resolução CD/ANPD nº 19/2024.

Foram utilizados quatro eixos de análise: caracterização da transferência, base jurídica invocada, grau de transparência informacional e mecanismos de garantia declarados. O método adotado buscou verificar a correspondência entre conformidade formal e efetividade material das garantias previstas na legislação brasileira.

APÊNDICE B – RESUMO VISUAL DOS APONTAMENTOS DA PESQUISA



Ilustração 3 - resumo visual dos apontamentos da pesquisa