PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO
GRADUAÇÃO EM DIREITO

VIKTOR ANDREAS BIONDO RITTER UND EDLER VON SCHMÄDEL

# A LEGISLAÇÃO APLICÁVEL PARA CASOS ENVOLVENDO A UTILIZAÇÃO INDEVIDA DE DADOS PESSOAIS DE TITULARES BRASILEIROS, POR OPERADORES SITUADOS NA UNIÃO EUROPÉIA, POR MEIO DE CLÁUSULAS-PADRÃO CONTRATUAIS CELEBRADAS POR CONTROLADOR SITUADO NO BRASIL

São Paulo
2025

**VIKTOR ANDREAS BIONDO RITTER UND EDLER VON SCHMÄDEL**

# A LEGISLAÇÃO APLICÁVEL PARA CASOS ENVOLVENDO A UTILIZAÇÃO INDEVIDA DE DADOS PESSOAIS DE TITULARES BRASILEIROS, POR OPERADORES SITUADOS NA UNIÃO EUROPÉIA, POR MEIO DE CLÁUSULAS-PADRÃO CONTRATUAIS CELEBRADAS POR CONTROLADOR SITUADO NO BRASIL

Trabalho de Conclusão de Curso apresentado à Pontifícia Universidade Católica de São Paulo como requisito parcial para a obtenção do título de Bacharel em direito.

Orientadora Prof.ª Dra. Marina Faraco

**São Paulo**

**2025**

VIKTOR ANDREAS BIONDO RITTER UND EDLER VON SCHMÄDEL

A LEGISLAÇÃO APLICÁVEL PARA CASOS ENVOLVENDO A UTILIZAÇÃO INDEVIDA DE DADOS PESSOAIS DE TITULARES BRASILEIROS, POR OPERADORES SITUADOS NA UNIÃO EUROPÉIA, POR MEIO DE CLÁUSULAS-PADRÃO CONTRATUAIS CELEBRADAS POR CONTROLADOR SITUADO NO BRASIL

APROVADO EM: __/__/____

BANCA EXAMINADORA

_____

(Orientador)

_____

(Avaliador)

_____

(Avaliador)

Dedico o presente trabalho à minha família, Silvia, Andreas e Ingrid, à Isabela, ao Gabriel S. e aos meus amigos e colegas de faculdade, que estiveram sempre ao meu lado durante a minha graduação.

VON SCHMÄDEL, Viktor Andreas Biondo Ritter und Edler. A Legislação Aplicável para Casos Envolvendo a Utilização Indevida de Dados Pessoais de Titulares Brasileiros, por Operadores Situados na União Europeia, por Meio de Cláusulas-Padrão Celebradas por Controlador Situado no Brasil. Trabalho de Conclusão de Curso (Graduação em Direito) – Pontifícia Universidade Católica de São Paulo – PUC-SP, 43p, 2025.

## RESUMO

O presente trabalho tem por objetivo analisar a legislação aplicável aos casos de utilização indevida de dados pessoais de titulares brasileiros por operadores situados na União Europeia, especialmente quando a transferência internacional de dados ocorre por meio de cláusulas-padrão contratuais celebradas por controlador localizado no Brasil. Diante da crescente globalização digital e da intensa circulação transnacional de informações, a pesquisa busca compreender de que forma as normas brasileiras e europeias interagem e se aplicam na proteção dos titulares de dados. Para tanto, adota-se o método dedutivo, com base em pesquisa bibliográfica e análise comparativa entre o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) e a Lei Geral de Proteção de Dados brasileira (LGPD), bem como da recente Resolução CD/ANPD nº 19/2024, que regulamenta a transferência internacional de dados e institui as cláusulas-padrão contratuais.

Os resultados obtidos indicam que, embora existam semelhanças estruturais entre a GDPR e a LGPD, especialmente quanto aos princípios e fundamentos da proteção de dados, há diferenças relevantes na determinação da legislação e da jurisdição aplicáveis em situações internacionais. A análise da Resolução CD/ANPD nº 19/2024 demonstra que, nas transferências realizadas por meio das cláusulas-padrão contratuais brasileiras, a legislação aplicável será a nacional, sob fiscalização da ANPD, reforçando a soberania jurídica do Brasil e a tutela dos titulares de dados. Contudo, para casos envolvendo cláusulas-padrão equivalentes, as partes poderão optar pela legislação mais adequada ao caso, não se restringindo à brasileira. Conclui-se, portanto, que a consolidação de mecanismos normativos claros e harmônicos entre diferentes ordenamentos é essencial para garantir segurança jurídica e efetiva proteção dos direitos fundamentais em um contexto globalizado.

**Palavras-chave:** Proteção de dados pessoais. Transferência internacional de dados. LGPD. GDPR. Cláusulas-padrão contratuais. Cláusulas-padrão equivalentes. ANPD.

**VON SCHMÄDEL, Viktor Andreas Biondo Ritter und Edler.** *The Applicable Legislation for Cases Involving the Improper Use of Personal Data of Brazilian Data Subjects by Operators Located in the European Union, Through Standard Contractual Clauses Concluded by a Controller Based in Brazil.* Undergraduate Thesis (Bachelor's Degree in Law) – Pontifical Catholic University of São Paulo – PUC-SP, 41p, 2025.

## ABSTRACT

This study aims to analyze the legislation applicable to cases involving the improper use of personal data belonging to Brazilian data subjects by operators located in the European Union, especially when the international transfer of data takes place through standard contractual clauses executed by a controller based in Brazil. In light of increasing digital globalization and the intense transnational flow of information, this research seeks to understand how Brazilian and European legal frameworks interact and apply to the protection of data subjects. To this end, the deductive method is adopted, supported by bibliographical research and a comparative analysis between the European Union's General Data Protection Regulation (GDPR) and Brazil's General Data Protection Law (LGPD), as well as the recent ANPD Resolution No. 19/2024, which regulates international data transfers and establishes standard contractual clauses.

The findings indicate that, although there are structural similarities between the GDPR and the LGPD—particularly regarding their principles and foundations of data protection—significant differences remain in determining the applicable law and jurisdiction in international scenarios. The analysis of ANPD Resolution No. 19/2024 shows that, in transfers carried out through Brazilian standard contractual clauses, the applicable legislation will be Brazilian law, under the supervision of the ANPD, reinforcing Brazil's legal sovereignty and the protection of data subjects. However, in cases involving equivalent standard contractual clauses, the parties may choose the law deemed most appropriate for the situation, not limited to Brazilian legislation. Therefore, it is concluded that the consolidation of clear and harmonized normative mechanisms among different legal systems is essential to ensure legal certainty and the effective protection of fundamental rights in a globalized context.

**Keywords:** Personal data protection. International data transfer. LGPD. GDPR. Standard contractual clauses. ANPD.

SUMÁRIO

## INTRODUÇÃO

O mundo está cada vez mais digital com o surgimento de novas tecnologias. Tarefas que, até então, demoravam horas para serem executadas, estão ficando mais fáceis de serem realizadas. Pessoas utilizam da tecnologia por longos períodos diariamente, seja para as suas atividades laborais ou para lazer.

Até o início dos anos 2000, a tecnologia ainda não era tão comum na vida das pessoas. Ainda que as pessoas já fizessem o uso do telefone como meio de comunicação, ainda não existiam celulares ou computadores com alto desempenho.

Em 25 de outubro de 2001, a empresa Microsoft, não tão grande à época, lançava o sistema operacional "Windows XP", que foi o responsável pela democratização do acesso à internet por grande parte da população. O sistema operacional foi utilizado em grande escala, até que, em 14 de abril de 2009, perdeu o seu suporte oficial da Microsoft, dando espaço para versões mais recentes, como o "Windows 7", "Windows 8" e o atual "Windows 11".

No campo das redes sociais, em 2004, foi criado, por Mark Zuckerberg, Dustin Moskovitz, Chris Hughes, Andrew McCollum e o brasileiro Eduardo Saverin, o Facebook. A rede social foi consolidada em grande escala em outros países para além dos Estados Unidos quando, em 2008, chegou ao Brasil.

Com o passar dos anos, o Facebook foi ganhando um grande papel mundial no campo das redes sociais. À medida em que a empresa foi expandindo, novos serviços e aplicativos foram sendo adquiridos, como o serviço Instagram, em 2012, e o aplicativo WhatsApp, em 2014. Hoje, a Meta Platforms, Inc. possui diversas empresas e serviços relacionados, sendo parte da rotina da maioria da população mundial.

Em 2010, foi popularizada, mundialmente, a computação em nuvem, com o surgimento de serviços como Dropbox e o Google Drive. Diversas pessoas passaram a armazenar os seus conteúdos na "nuvem", ao invés de ter um *Hard Disk* ("HD") disponível para o salvamento dos conteúdos.

O período da pandemia, entre 2019 e 2021, também foi um ponto de destaque para o desenvolvimento de novos serviços ou o seu aprimoramento, como a realização de reuniões telepresenciais ou o chamado "Home Office", permitindo o trabalho totalmente remoto ou híbrido.

Atualmente, estão cada vez mais presentes no dia a dia tecnologias de Inteligência Artificial ("IA") e *machine learning*. Além disso, no campo das telecomunicações, a evolução da 3G de redes móveis para a 4G e, posteriormente, 5G é de suma importância para que os sistemas operacionais possam atuar com mais velocidade.

Muitas das tecnologias que surgiram ao longo dos anos contam com a utilização de dados dos seus usuários para o funcionamento. A coleta de dados, a sua disponibilização e o uso são regulamentados por diversas normas, as quais, não obstante a sua recente redação, são vitais para a tutela dos usuários.

Além disso, com o mundo cada vez mais globalizado, ou seja, os países cooperando para o desenvolvimento tecnológico, o uso e compartilhamento de dados também desempenham uma função importante. Seja no campo das tecnologias desenvolvidas para o lazer, como redes sociais, ou no campo das tecnologias desenvolvidas para operações profissionais e até militares, o compartilhamento de dados é fundamental para o seu funcionamento.

Os exemplos podem ser encontrados nas situações mais corriqueiras: ao realizar uma compra em um *site* estrangeiro, o qual está hospedado em outro país, haverá a transferência internacional dos dados do consumidor. Outra ocasião comum envolvendo a transferência internacional de dados é o armazenamento de documentos em serviços como Dropbox, Amazon AWS ou Google Drive. Neste segundo exemplo, o usuário envia o documento e, consequentemente, seus dados, os quais serão armazenados em servidores estrangeiros.

Empresas multinacionais também podem fazer uso da transferência internacional de dados para o seu funcionamento. Uma corporação, cuja sede se encontra na União Europeia, por exemplo, e possui uma filial no Brasil, poderá compartilhar os dados dos seus funcionários, internamente, para o seu devido funcionamento.

Evidentemente, a transferência internacional de dados é de grande importância para o desenvolvimento tecnológico mundial. No entanto, ao mesmo tempo em que traz grandes benefícios, a transferência internacional de dados também carrega consigo uma grande responsabilidade.

Não é raro escutar falar de "vazamentos de dados" em grandes empresas. Ataques *hackers* – pessoas de má-fé cujo objetivo é se infiltrar em sistemas internos de empresas, coletar os dados dos usuários ilicitamente e, posteriormente, vazá-los – estão cada vez mais comuns. Em que pesem as empresas empreguem diversas tecnologias a coibir esse tipo de

ação, adotando sistemas de evolução constante da segurança, nenhuma tecnologia está imune a ataques de terceiros.

A fim de coibir esse tipo de ação, é de suma importância a edição de normas que protejam o titular dos dados, possibilitando um espaço seguro para a sua utilização. Essa proteção dos dados não deverá ser restrita ao país, mas deve abranger todos os sujeitos envolvidos, estejam eles no Brasil ou em outro país.

A questão recai sobre como é possível fornecer a todos os envolvidos segurança jurídica suficiente, para que, caso haja um vazamento de dados, possam ser tomadas as devidas medidas, frente aos tribunais competentes para julgar a demanda.

Para a aplicação correta da norma aplicável ao caso, deve-se, de início, identificar quais são os sujeitos integrantes de uma transferência de dados. Para isso, destacam-se três agentes principais, cuja descrição cristalina extrai-se da Lei Geral de Proteção de Dados ("LGPD") (BRASIL, 2018), a saber:

- **Titular dos dados**: pessoa natural cujos dados serão objetos de tratamento;

- **Controlador**: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento dos dados pessoais dos titulares; e

- **Operador**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Após a identificação clara de todos os envolvidos em uma operação de tratamento de dados, pode-se analisar qual a legislação aplicável para tutelar o direito deles, em especial, do titular dos dados.

Os países contam com diferentes legislações aplicáveis para a proteção dos dados. No Brasil, por exemplo, aplica-se a LGDP, Lei Federal que 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*"[1] (BRASIL, 2018).

[1] Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em:06/09/2025 .

Já na União Europeia, os sujeitos envolvidos no tratamento de dados de qualquer natureza estão protegidos pelo *General Data Protection Regulation* ("GDPR"), "*relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*"[2] (EUROPEAN UNION, 2016).

A questão que se busca responder por meio do presente trabalho é qual é a legislação aplicável para casos envolvendo a utilização indevida de dados pessoais de titulares brasileiros, por operadores situados na União Europeia, por meio de cláusulas-padrão celebradas por controlador situado no Brasil.

Para isso, serão exploradas ambas as legislações, tanto a GDPR quanto a LGPD, as suas disposições e conceitos, bem como a recente editada Resolução nº 19, de 23 de agosto de 2024, e aprovada pelo Ministério da Justiça e Segurança Pública e pela Agência Nacional de Proteção de Dados ("ANPD"). Também serão exploradas as três formas de transferência de dados, a saber, por meio de decisão de adequação, garantias contratuais apropriadas e exceções específicas, com foco na utilização de cláusula-padrão.

Portanto, diante do cenário apresentado, observa-se que o avanço tecnológico e a crescente digitalização das relações sociais e profissionais intensificaram a coleta, o uso e o compartilhamento de dados pessoais em escala global. A transferência internacional de dados, antes restrita a operações específicas, tornou-se parte integrante da rotina de milhões de usuários, exigindo atenção redobrada quanto à sua segurança e à proteção jurídica dos titulares envolvidos. Nesse contexto, a regulamentação adequada surge como elemento essencial para garantir que os benefícios da tecnologia não sejam ofuscados por riscos à privacidade e à integridade dos dados.

A crescente incidência de vazamentos e ataques cibernéticos evidencia a necessidade de normas robustas e eficazes, capazes de proteger os dados pessoais independentemente da localização geográfica dos agentes envolvidos. A harmonização entre legislações nacionais e internacionais, como a LGPD no Brasil e a GDPR na União Europeia, revela-se fundamental para assegurar segurança jurídica e promover a confiança dos usuários nas plataformas digitais. A atuação coordenada entre países e órgãos reguladores é, portanto, indispensável para enfrentar os desafios impostos pela globalização digital.

Este trabalho, ao se debruçar sobre os aspectos legais da transferência internacional de dados entre Brasil e União Europeia, busca contribuir para a compreensão das normas

[2] "The protection of natural persons with regard to the processing of personal data and on the free movement of such data."

aplicáveis e dos mecanismos de proteção existentes. A análise das legislações, das cláusulas-padrão permitirá identificar os caminhos possíveis para garantir a tutela dos titulares de dados, especialmente em situações internacionais, identificando a legislação aplicável para caso de litígio.

# 1. LEGISLAÇÃO EUROPEIA DE PROTEÇÃO DE DADOS REFERENTES À TRANSFERÊNCIA INTERNACIONAL DE DADOS

## 1.1 Legislação Europeia: Regulamento Geral sobre Proteção de Dados

Os países integrantes da União Europeia contam com uma legislação específica para a proteção dos dados dos seus titulares. Não suficiente, a GDPR também proporciona segurança jurídica para as outras partes da relação, como os operadores e os controladores.

Para compreender a estrutura e a importância da GDPR nos dias de hoje, deve-se olhar para o passado e analisar o histórico da proteção de dados no mundo.

Entre os anos de 1933 e 1945, a Alemanha passava pelo regime nazista, o qual foi oficializado em 1943, no chamado Terceiro Reich. Nesse período, o Partido Nacional-Socialista dos Trabalhadores (NSDAP), controlado por Adolf Hitler, tinha o controle da nação alemã.

Esse período foi marcado por crimes contra a humanidade praticados pelos nazistas. Não à toa, para conseguir se manter no poder e seguir controlando a Alemanha, em especial durante o período da Segunda Guerra Mundial, o governo de Hitler precisava ter total controle da população, não apenas subjetivamente, por meio da ideologia, como também objetivamente, por meio do controle total das pessoas.

Um Estado autoritário e ditatorial, como a Alemanha nesse período, precisa contar com diversos mecanismos para a sua manutenção, como o controle de informações de toda a população. Para isso, o país contou com diferentes órgãos estatais criados para o controle de informações das pessoas, como a *Geheime Staatspolizei*, polícia secreta que atuava no Estado. O controle da informação era vital para o regime nazista, de modo que, quanto mais se soubesse, mais controle possuiriam sobre a população.

Com o fim da Segunda Guerra Mundial e a supressão do regime autoritário nazista, a Alemanha passou a ter um olhar mais crítico à vigilância dos dados da população, de modo a impedir que fossem realizadas novas manobras políticas-ditatoriais no país.

Em 1949 foi editada a *Grundgesetz* (tradução livre: Lei Fundamental Alemã), por meio da qual foram colocados em pauta os limites entre as atividades administrativas e a proteção de dados pessoais. Em que pese não haja uma menção explícita a respeito da proteção de

dados da população, pode-se extrair diversos trechos que, indiretamente, protegem os dados das pessoas.

Por meio do artigo 1º da *Grundgesetz*, está previsto que "*a dignidade humana é inviolável. Respeitá-la e protegê-la é dever de todas as autoridades estatais*"[3] (ALEMANHA, 1949, tradução livre). Além disso, por meio do artigo 2º, está previsto que "*toda pessoa tem direito ao livre desenvolvimento da sua personalidade, desde que não viole os direitos dos outros e não ofenda a ordem constitucional nem a lei moral*"[4] (ALEMANHA, 1949, tradução livre).

É evidente a preocupação da Alemanha em garantir à sua população o direito à autodeterminação informacional. Como bem definido por José Marcelo M. Vigliar (VIGLIAR 2025), o direito à autodeterminação informacional traduz-se como "*um desmembramento do direito à privacidade, visando essencialmente tutelar de forma efetiva os dados/informações pessoais das pessoas naturais garantindo-lhes o controle sob eles, sendo, portanto, imperiosa a necessidade de seu reconhecimento como um novo direito fundamental*".

Também na norma *Grundgeset* está previsto que o lar será inviolado, por meio do artigo 13[5]. Ainda que não faça uma menção direta à proteção dos dados pessoais da população, é evidente a preocupação da norma em garantir o direito à propriedade privada, de modo que a pessoa não poderá sofrer intrusões indevidas em sua vida, podendo ser interpretado, *latu sensu*, no âmbito das suas informações pessoais.

Anos após, o Estado alemão editou a primeira lei do mundo a reconhecer, expressamente, o direito à proteção de dados, a *Hessisches Datenschutzgestz*, atualmente chamada de *Hessisches Datenschutz- und Informationsfreiheitsgesetz*, a qual está vigente até os dias de hoje, havendo passado por diversas modificações ao longo dos anos, e se aplica "*ao tratamento de dados pessoais por autoridades públicas do Estado, municípios e distritos*"[6] (ALEMANHA, 1970, tradução livre).

[3] "Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt."

[4] "Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt."

[5] Die Wohnung ist unverletzlich."

[6] "Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch die öffentlichen Stellen des Landes, der Gemeinden und Landkreise"

Exatamente com o espírito de tutela aos titulares dos dados, por meio do artigo 42 da *Hessisches Datenschutz- und Informationsfreiheitsgesetz*, foram estabelecidos os princípios norteadores do processamento e utilização de dados, a saber:

> Os dados devem ser: 1. processados de forma legal e justa; 2. processados para fins específicos, explícitos e legítimos e não tratados de forma incompatível com esses fins; 3. adequados à finalidade do tratamento, relevantes e não excessivos à finalidade do tratamento; 4. precisos e, quando necessário, mantidos atualizados; serão tomadas todas as medidas razoáveis para que os dados pessoais imprecisos sejam apagados ou retificados sem demora; 5. conservados apenas pelo prazo necessário à finalidade dos dados; 6. processados de forma que se assegure a adequada segurança dos dados pessoais, incluindo proteção contra acesso não autorizado ou acidental e contra destruição, perda, alteração ou divulgação não autorizada, usando medidas técnicas e organizacionais apropriadas. (ALEMANHA 1970).

Na Suécia, em 11 de maio de 1973, foi promulgada a *Datalagen*, (Lei de Dados da Suécia), a qual entrou em vigor em 1º de julho de 1974. A legislação entrou em vigor após a Segunda Guerra Mundial, período que, como visto anteriormente, foi marcado por uma crescente preocupação com o uso de computadores para armazenar informações pessoais da população.

Entre os principais pontos da *Datalagen* estavam a exigência de licenças para sistemas que processassem dados pessoais, emitidas pela Autoridade Sueca de Proteção de Dados (*Data Inspection Board*). A lei também garantia o direito de acesso dos indivíduos às suas informações e impunha restrições à exportação de dados para fora do país, exigindo autorização específica – destaque para esse ponto, uma vez que, pela primeira vez em uma legislação, a transferência internacional de dados foi tutelada. Embora inovadora, a legislação foi considerada complexa e de difícil aplicação, especialmente no que diz respeito ao registro de dados e ao fluxo internacional de informações, o que levou a diversas emendas ao longo dos anos.

Com o passar do tempo, a *Datalagen* tornou-se obsoleta frente às novas tecnologias e à evolução da legislação europeia. Após a adesão da Suécia à União Europeia em 1995, foi iniciada uma revisão completa da lei, culminando na substituição da *Datalagen* pela Lei de Dados Pessoais (*Personuppgiftslagen*) em 1998, alinhada à Diretiva Europeia de Proteção de Dados.

Posteriormente à *Datalagen*, foi iniciada a segunda geração de proteção de dados, marcada pelo surgimento da Diretiva 95/46/CE, também denominada Diretiva Europeia de Proteção de Dados, a qual foi editada em 1995 pelo Parlamento Europeu e pelo Conselho da União Europeia, representando um marco normativo na tutela dos direitos fundamentais relacionados à privacidade e à proteção de dados pessoais.

Seu propósito central foi harmonizar as legislações internas dos Estados-membros, de modo a assegurar simultaneamente a livre circulação de informações no espaço comunitário e a salvaguarda dos direitos dos titulares. Para isso, a norma estabeleceu conceitos jurídicos fundamentais, como "dados pessoais" e "tratamento de dados", bem como fixou requisitos para a obtenção do consentimento, a determinação de finalidades específicas para o tratamento e a responsabilização dos controladores (UNIÃO EUROPEIA, 1995).

De forma inovadora, a Diretiva 95/46/CE determinou a exigência de criação de autoridades nacionais de controle independentes – o que, mais tarde, seria introduzido à legislação brasileira, por meio da criação da Agência Nacional de Proteção de Dados ("ANPD") -, incumbidas da fiscalização e da aplicação das regras previstas, além de garantir aos indivíduos prerrogativas essenciais, tais como o direito de acesso, retificação e exclusão de seus dados.

A norma buscou, assim, equilibrar os interesses econômicos relacionados ao fluxo informacional e a necessidade de tutela da esfera privada dos cidadãos, consolidando um patamar mínimo de proteção em nível europeu. Tal equilíbrio revelou-se essencial para a construção do mercado interno, ao estabelecer maior segurança jurídica para as operações que envolvem o tratamento transfronteiriço de dados, o que seria, posteriormente, incorporado à *General Data Protection Regulation* ("GDPR").

Anos após, em maio de 2018, entrou em vigor a GDPR, dando início à terceira geração de legislações de proteção de dados. A GDPR substituiu, em escala global e, principalmente, na União Europeia, a aplicação da Diretiva 95/46/CE, introduzindo uma abordagem holística e proativa à privacidade de dados.

Louise S. H. Thomaz da Silva muito bem explica a importância da edição da GDPR, introduzindo o direito à proteção de dados como um direito fundamental (SILVA., 2021). Confira-se:

> "Diante desse cenário, governos passaram a tomar medidas para que empresas aumentassem os investimentos com a segurança dos dados dos usuários. A União Europeia criou, em 2016, uma nova regulamentação para proteção de dados

> pessoais: a General Data Protection Regulation 2016/679 (GDPR) (UNIÃO EUROPEIA, 2016). Tal instrumento legal foi um importante marco para proteção e privacidade de dados dos cidadãos da União Europeia e do espaço Econômico Europeu. Por meio dele, a proteção de dados pessoais passou a ser tratada como direito fundamental (BISSO et al., 2020)".

Para além das suas disposições, a GDPR foi essencial para a criação de diversas outras leis ao redor do mundo, representando um modelo de inovação e proteção jurisdicional aos dados da população dos países.

Dentre os diversos dispositivos trazidos pela lei, destaca-se o capítulo V, por meio do qual estão dispostas as normas referentes às "*Transferências de dados pessoais para países terceiros ou organizações internacionais*", as quais serão objeto do presente estudo.

### 2.1.1 Requisitos aplicáveis para a transferência internacional de dados

Como visto, a GDPR é o Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 "*relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*" (UNIÃO EUROPEIA, 2016).

O texto normativo é dividido em sete capítulos, tratando, cada um deles, sobre determinados aspectos e direitos referentes à proteção de dados. A transferência internacional de dados, por sua vez, é abordada ao longo do capítulo V, o qual será objeto central do presente trabalho.

Contudo, antes de adentrar no capítulo V especificamente, deve-se explorar alguns objetivos e conceitos da Lei, para que fiquem mais claras e de melhor compreensão as conclusões do presente estudo.

Através do artigo 1º, capítulo I, da GDPR, estão fixados o objeto e os objetivos que o legislador pretendeu alcançar por meio da Lei. A saber:

> "1. O presente regulamento estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
>
> 2. O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais.

> 3. A livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais." (UNIÃO EUROPEIA, 2016)

Ora, é evidente que o tratamento internacional de dados deve sempre ter como princípios o da livre circulação de dados, a fim de fomentar o desenvolvimento econômico da região, mas sempre respeitando os direitos e as liberdades fundamentais das pessoas singulares, em especial, o seu direito à proteção dos dados pessoais.

Assim, ao expressamente consignar os referidos princípios e direitos na norma, o legislador evidentemente preferiu pela proteção da pessoa humana, mas sem deixar com que a livre iniciativa e a economia regional pudesse ser afetadas, de modo que deverá sempre haver um equilíbrio entre as liberdades e direitos individuais e o tratamento de dados pelas empresas e entes que empreguem a União Europeia.

Adiante, por meio do artigo 3º da GDPR, foi estabelecida a territorialidade de aplicação da norma, abrangendo, inclusive, casos em que há tratamento internacional dos dados. Para tal, a Lei será aplicada tanto quando o responsável pelo tratamento ou um subcontratante estiverem situados no território da União Europeia, quanto quando o titular dos dados pessoais residir na União Europeia, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União Europeia. Confira-se:

> "1. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União.
> 2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:
> a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento;
> b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União." (UNIÃO EUROPEIA, 2016)

Por meio do artigo 4º da GDPR, estão estabelecidas as definições utilizadas na norma, ou seja, palavras-chave cuja classificação é de suma importância para o entendimento da

Lei. Para o presente trabalho, vamos explorar algumas classificações importantes ao tratamento internacional de dados. A saber:

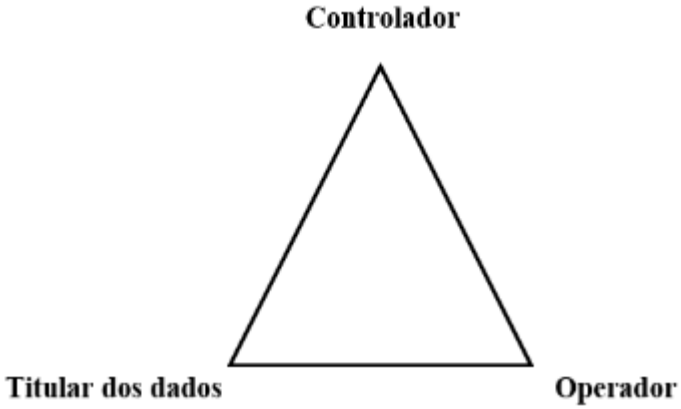
> "1) «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;
>
> 2) «Tratamento», uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;
>
> (...)
>
> 7) «Responsável pelo tratamento», a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro;
>
> 8) «Subcontratante», uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes;
>
> 10) «Terceiro», a pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais;" (UNIÃO EUROPEIA, 2016)

Nesse ponto, já se encontra o primeiro ponto de discussão e análise internacional. Para fins de comparação, pode-se equiparar o conceito de "responsável pelo tratamento" da GDPR ao conceito de "controlador" da LGPD, ou seja, pessoa física ou jurídica que determina o tratamento de dados, bem como define os critérios específicos. Além disso, o "controlador" e o "responsável pelo tratamento" são os que tomam as decisões de como (*latu sensu*) será

realizado o tratamento dos dados – para todos os fins e no intuito de facilitar a compreensão, a partir desse momento, considera-se este ente como "controlador", para ambas as legislações.

Por outro lado, a GDPR classifica como "subcontratante" aquele que, por conta do controlador, trate os dados pessoais. Semelhança maior não há com a figura do "operador" da LGPD, o qual é responsável pelo tratamento de dados pessoais em nome do controlador – novamente, para todos os fins e no intuito de facilitar a compreensão, a partir desse momento, considera-se este ente como "operador", para ambas as legislações.

Portanto, a cadeia de relacionamento em ambas as legislações é composta por três personagens principais. A saber:




Relembrando o quanto disposto por meio do artigo 3º, da GDPR, item 1, denota-se que a referida Lei será aplicada para casos em que o "estabelecimento" do controlador ou do operador esteja situado na União Europeia, independentemente de os dados terem sido tratados na União Europeia.

Portanto, seria a GDPR aplicável para todos os casos que envolvam a transferência internacional de dados, nos quais o controlador e/ou controlador estejam situados na União Europeia? Depende. De acordo com o título 1º, artigo 3º, item 1, sim, seria a legislação aplicável. No entanto, há situações em que a GDPR não poderia ser a base legal para a resolução do conflito, mas sim a LGDP.

Em que pese 50% da pergunta norteadora do presente trabalho – qual é a legislação aplicável para casos envolvendo a utilização indevida de dados pessoais no contexto Brasil-Europa - já tenha sido respondida, para chegar à totalidade da resposta, deve-se se debruçar sobre os demais dispositivos da Lei.

A partir do capítulo V, são tratadas todas as disposições para a transferência internacional de dados, utilizando como base os fundamentos anteriormente mencionados. O capítulo V é introduzido da seguinte maneira:

> "Qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional só é realizada se, sem prejuízo das outras disposições do presente regulamento, as condições estabelecidas no presente capítulo forem respeitadas pelo responsável pelo tratamento e pelo subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional. Todas as disposições do presente capítulo são aplicadas de forma a assegurar que não é comprometido o nível de proteção das pessoas singulares garantido pelo presente regulamento." (UNIÃO EUROPEIA, 2016)

O legislador, ao editar a GDPR, teve uma grande preocupação com a segurança jurídica e material dos dados, garantindo ao titular que haverá um nível de proteção mínimo praticado pelos controladores e operadores.

Para isso, a Comissão Europeia ("Comissão") deverá decidir se um país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Para esses casos, a transferência internacional de dados não exigirá autorização específica.

Para casos em que o país não atenda às disposições anteriores, ou seja, casos em que a Comissão não tenha aprovado o nível de segurança adequado do país, a transferência internacional de dados estará sujeita à apresentação de garantias adequadas, para que assim os controladores ou operadores possam transferir os dados dos seus usuários, nos termos do artigo 46º, item 1, da GDPR.

As medidas adequadas estão previstas por meio do artigo 46º, item 2, da GDPR, no qual há seis formas de transferência internacional de dados, sem requerer nenhuma autorização específica de uma autoridade de controle. A saber:

> "2. Podem ser previstas as garantias adequadas referidas no n.o 1, sem requerer nenhuma autorização específica de uma autoridade de controlo, por meio de:
> a) Um instrumento juridicamente vinculativo e com força executiva entre autoridades ou organismos públicos;

> b) Regras vinculativas aplicáveis às empresas em conformidade com o artigo 47.o;
> c) Cláusulas-tipo de proteção de dados adotadas pela Comissão pelo procedimento de exame referido no artigo 93.o, n.o 2;
> d) Cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo e aprovadas pela Comissão pelo procedimento de exame referido no artigo 93.o, n.o 2;
> e) Um código de conduta, aprovado nos termos do artigo 40.o, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados; ou
> f) Um procedimento de certificação, aprovado nos termos do artigo 42.o, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados." (UNIÃO EUROPEIA, 2016)

É evidente que, se um país não contar com o nível de proteção adequado para que seja realizada a transferência internacional de dados da forma como prevista por meio do artigo 45, item 3, da GDPR, não será um impeditivo total para que ocorra a transferência. Pelo contrário, foram previstas outras formas diferentes de se realizar a transferência internacional de dados, observando o nível de segurança de cada caso em específico.

O item 3 do artigo 46 também prevê que, para a hipótese do tratamento de dados não se encaixar nas opções anteriores, o controladoR e/ou o operador, sob autorização da "autoridade de controle competente" poderá estabelecer cláusulas contratuais com os titulares dos dados de país terceiro. Além disso, está previsto que poderão ser celebrados acordos internacionais administrativos entre as autoridades ou organismos públicos que contemplem os direitos efetivos e oponíveis dos titulares dos dados.

Portanto, nos termos da GDPR, para que uma transferência internacional de dados possa ser realizada e efetivada legalmente, o controlador deverá escolher entre **(i)** uma decisão de adequação, caso tenha sido concedida pela Comissão, **(ii)** garantias adequadas e elencadas no artigo 46 da GDPR ou **(iii)** derrogações específicas, como o consentimento explícito dado pelo titular para a realização da transferência.

Conforme mais bem detalhado por Matheus Passos Filho (SILVA, 2021), há uma hierarquia entre as opções mencionadas anteriormente, a qual deverá ser analisada e respeitada na hora de se escolher entre as diversas maneiras de transferência internacional de dados. Confira-se:

> “Reforce-se aqui que essas bases legais devem ser escolhidas de maneira hierárquica. Significa dizer que um agente de tratamento, ao buscar realizar uma transferência internacional, deverá em primeiro lugar verificar se o país destinatário já possui um decisão de adequação pela Comissão Europeia. Caso não exista uma decisão de adequação, deverá então optar por uma das garantias adequadas do art. 46, e só em última instância é que deverá se utilizar de uma das derrogações específicas indicadas no art. 49 do Regulamento.
>
> Por outro lado, é importante lembrar que quanto mais se desce nessa hierarquia, maiores são os riscos para o titular. Isso porque as garantias adequadas não podem fornecer proteção contra certos riscos inerentes à proteção de dados que devem ser levados em consideração quando uma decisão de adequação é emitida. Por exemplo, uma decisão de adequação avalia o risco de acesso aos dados pelas autoridades públicas do país para o qual os dados são transferidos, o que não necessariamente ocorre quando o agente de tratamento se utiliza de um simples contrato com o agente de tratamento do país terceiro. Além disso, as disposições do art. 46 do RGPD devem ser lidas à luz da Carta dos Direitos Fundamentais da União Europeia, uma vez que, como o TJUE constatou, a aplicabilidade do direito da União implica a aplicabilidade da Carta – o que aumenta o nível de exigência em relação aos agentes de tratamento quando estes utilizam uma base legal que não uma decisão de adequação da Comissão Europeia. As derrogações, por sua vez, não garantem em absoluto qualquer tipo de proteção extra aos dados.” (SILVA, 2021)

Em síntese, a GDPR consolidou-se como um marco normativo de referência global ao estabelecer um sistema robusto e detalhado para a proteção de dados pessoais, fundamentado na harmonização entre a livre circulação de informações e a tutela dos direitos fundamentais dos indivíduos. O regulamento buscou não apenas garantir segurança jurídica e transparência nas relações entre titulares, controladores e operadores, mas também fundamentar um ambiente de confiança que favorece o desenvolvimento econômico e tecnológico dentro e fora da União Europeia. Dessa forma, ao fixar princípios claros e mecanismos precisos para o tratamento e a transferência internacional de dados, a GDPR reforça a centralidade da dignidade da pessoa humana e da autodeterminação informativa como pilares do direito europeu contemporâneo.

Por conseguinte, a hierarquização dos instrumentos de transferência internacional – das decisões de adequação às derrogações específicas – evidencia a preocupação do legislador europeu em assegurar níveis graduais e proporcionais de proteção, conforme o grau de risco envolvido. Assim, o regulamento não apenas define regras técnicas, mas estabelece uma

base para a análise comparativa com a LGPD e para a compreensão das interações jurídicas entre Brasil e União Europeia no contexto das transferências internacionais de dados.

### 2.1.2 Cláusulas-tipo

Antes de se analisar a aplicação da LGPD e da GDPR para casos envolvendo a transferência internacional de dados, deve-se aprofundar o estudo em uma forma específica de realização da transferência, qual seja, a transferência internacional de dados por meio de cláusulas-tipo celebradas entre as partes.

Conforme visto, antes de se efetivar o tratamento dos dados, o controlador e/ou o operador deverão escolher, hierarquicamente, entre três maneiras distintas de se conseguir a devida autorização legal, conforme mais bem descritas anteriormente.

Para o Brasil, contudo, o controlador e/ou o operador não poderão escolher a transferência internacional de dados através da decisão de adequação. Isso porque o Brasil não está entre os países indicados pela Comissão como seguros para a realização da transferência internacional de dados, cuja lista inclui: Andorra, Argentina, Canadá, Ilhas Faroé, Guernsey, Israel, Ilha de Man, Japão, Jersey, Nova Zelândia, República da Coreia, Suíça, Reino Unido, Estados Unidos e o Uruguai[7].

Uma vez que o Brasil não está na lista de países aprovados pela União Europeia para a transferência internacional de dados por meio de decisão de adequação, a via eleita para que a transferência seja válida deverá ser das garantias adequadas ou das derrogações específicas.

Seguindo a linha hierárquica, a próxima alternativa disponível para o tratamento dos dados em escala internacional é a das garantias adequadas, prevista por meio do artigo 64, item 2 da GDPR.

Destaque-se que, dentre as seis opções de garantias adequadas, está prevista a de "cláusulas-tipo". Essa forma de transferência prevê que será garantia adequada de segurança, sem requerer nenhuma autorização específica de uma autoridade de controle, por meio de "*Cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo e aprovadas pela Comissão pelo procedimento de exame referido no artigo 93.o, n.o 2*" (UNIÃO EUROPEIA, 2016).

[7] Disponível em: https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_pt

As cláusulas contratuais-tipo (ou, simplesmente, "cláusulas-tipo") são caraterizadas por um conjunto de cláusulas padronizadas e que permitem aos exportadores de dados fornecer salvaguardas adequadas, ou seja, garantias jurídicas suficientes para assegurar que os dados pessoais transferidos para países terceiros sejam tratados em conformidade com os princípios e direitos previstos na legislação de proteção de dados aplicável.

A partir de 4º de junho de 2021, a Comissão proferiu uma decisão para a utilização de cláusulas-tipo, as quais já haviam sido pré-aprovadas. Ademais, por meio da referida decisão, a Comissão disponibilizou um modelo de contrato a ser adotado. Confira-se as disposições gerais da decisão:

> "Article 1
>
> 1. The standard contractual clauses set out in the Annex are considered to provide appropriate safeguards within the meaning of Article 46(1) and (2)(c) of Regulation (EU) 2016/679 for the transfer by a controller or processor of personal data processed subject to that Regulation (data exporter) to a controller or (sub-)processor whose processing of the data is not subject to that Regulation (data importer).
>
> 2. The standard contractual clauses also set out the rights and obligations of controllers and processors with respect to the matters referred to in Article 28(3) and (4) of Regulation (EU) 2016/679, as regards the transfer of personal data from a controller to a processor, or from a processor to a sub-processor.
>
> Article 2
>
> Where the competent Member State authorities exercise corrective powers pursuant to Article 58 of Regulation (EU) 2016/679 in response to the data importer being or becoming subject to laws or practices in the third country of destination that prevent it from complying with the standard contractual clauses set out in the Annex, leading to the suspension or ban of data transfers to third countries, the Member State concerned shall, without delay, inform the Commission, which will forward the information to the other Member States.
>
> Article 3
>
> The Commission shall evaluate the practical application of the standard contractual clauses set out in the Annex on the basis of all available information, as part of the periodic evaluation required by Article 97 of Regulation (EU) 2016/679."[8] (UNIÃO EUROPEIA, 2021)

[8] Tradução livre do autor:
Artigo 1
1. As cláusulas contratuais-tipo estabelecidas no Anexo são consideradas como garantias adequadas nos termos do artigo 46(1) e (2)(c) do Regulamento (UE) 2016/679 para a transferência, por um controlador ou operador, de dados pessoais tratados sob esse regulamento (exportador de dados) para um controlador

Assim, o legislador se preocupou em proporcionar a quem quer que deseje realizar a transferência internacional de dados entre a União Europeia e outro país sem uma decisão de adequação um modelo de contrato de clausulas-tipo a ser utilizado.

Conforme será mencionado e estudado posteriormente, o modelo europeu de contrato de cláusulas-tipo em muito se assemelha com o quanto previsto por meio da Resolução CD/ANPD nº 19, de 23 de agosto de 2024.

Contudo, antes de se adentrar na legislação brasileira sobre o tema, deve-se analisar mais a fundo o modelo de contrato de cláusulas-tipo anteriormente mencionado.

A decisão proferida pela Comissão, anteriormente descrito, prevê quatro modelos de contratos, quais sejam, para a utilização da transferência de dados do (i) controlador ao controlador, (ii) controlador ao operador, (iii) operador ao operador e (iv) operador ao controlador.

Para fins de especificação no presente estudo, será considerado à analise apenas o modelo estabelecido da transferência de dados do operador (situado na União Europeia) ao controlador (situado no Brasil), de forma a contribuir para a resposta à pergunta "qual é a legislação aplicável para casos envolvendo a utilização indevida de dados pessoais de titulares brasileiros, por operadores situados na união europeia, por meio de cláusulas-padrão contratuais celebradas por controlador situado no brasil?".

Conforme o modelo disponibilizado pela Comissão, a legislação aplicável para a transferência internacional de dados do operador ao controlador será aquela especificada entre as partes por meio do contrato celebrados. Confira-se: "*These Clauses shall be*

---

ou (sub)operador cuja atividade de tratamento dos dados não esteja sujeita ao referido regulamento (importador de dados).

2. As cláusulas contratuais-tipo também estabelecem os direitos e obrigações de controladores e operadores com relação aos temas tratados nos artigos 28(3) e (4) do Regulamento (UE) 2016/679, no que diz respeito à transferência de dados pessoais de um controlador para um operador, ou de um operador para um suboperador.

Artigo 2

Quando as autoridades competentes dos Estados-Membros exercerem poderes corretivos nos termos do artigo 58 do Regulamento (UE) 2016/679 em resposta ao fato de o importador de dados estar ou vir a estar sujeito a leis ou práticas no país terceiro de destino que o impeçam de cumprir as cláusulas contratuais-tipo estabelecidas no Anexo, levando à suspensão ou proibição das transferências de dados para países terceiros, o Estado-Membro em questão deverá, sem demora, informar a Comissão, que encaminhará a informação aos demais Estados-Membros.

Artigo 3

A Comissão avaliará a aplicação prática das cláusulas contratuais-tipo estabelecidas no Anexo com base em todas as informações disponíveis, como parte da avaliação periódica exigida pelo artigo 97 do Regulamento (UE) 2016/679.

*governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (specify country)*"[9](UNIÃO EUROPEIA, 2021).

Da mesma, diferentemente do quanto previsto para a transferência de dados do controlador ao controlador, do controlador ao operador e do operador ao operador, para a situação da transferência do dado entre o operador para o controlador, as partes poderão escolher a jurisdição e o foro aplicável ao caso. Confira-se: "*Any dispute arising from these Clauses shall be resolved by the courts of _____ (specify country)*"[10] (UNIÃO EUROPEIA, 2021).

Portanto, para casos em que envolvam a transferência internacional de dados entre um operador situado na União Europeia e um controlador estrangeiro, como situado no Brasil, a legislação e o foro aplicável para a solução de quaisquer demandas poderão ser estabelecidos pelas partes do contrato.

Contudo, mais especificamente em relação ao caso sob análise, de qual seria a legislação aplicável para a transferência internacional de dados entre operador situado na União Europeia e controlador situado no Brasil, a LGDP possui papel importante de estudo, contribuindo para a solução do conflito entre legislações.

[9] Tradução do autor: Estas cláusulas serão regidas pela lei de um país que permita direitos de terceiros beneficiários. As Partes concordam que esta será a lei de _____ (especificar o país).

[10] Tradução do autor: Qualquer litígio decorrente destas Cláusulas será resolvido pelos tribunais de _____ (especificar o país).

# 2. CONFLITOS ENVOLVENDO A UTILIZAÇÃO INDEVIDA DE DADOS PESSOAIS DE TITULAR E CONTROLADOR BRASILEIROS, POR OPERADOR SITUADO NA UNIÃO EUROPEIA, E A LEGISLAÇÃO APLICÁVEL

## 2.1 Legislação Brasileira

O Direito Internacional desempenha papel central na análise de situações em que há o envolvimento de diferentes ordenamentos jurídicos, especialmente quando o objeto do conflito transcende as fronteiras brasileiras.

No âmbito da proteção de dados pessoais, o Direito Internacional se revela ainda mais relevante, pois o fluxo informacional entre países impõe a necessidade de compatibilização entre legislações de diferentes países. A crescente relação entre sistemas jurídicos — impulsionada pela atuação de empresas multinacionais — exige que os Estados desenvolvam mecanismos que garantam a proteção dos titulares, sem inviabilizar as trocas comerciais e tecnológicas, em atenção ao princípio da liberdade econômica.

Assim, as regras de conexão e os princípios de cooperação internacional assumem papel determinante para definir qual legislação deve reger os conflitos que envolvem o tratamento e a transferência internacional de dados.

No caso específico das relações entre o Brasil e a União Europeia, a aplicação do direito internacional privado brasileiro ganha destaque, especialmente à luz da Lei de Introdução às Normas do Direito Brasileiro ("LINDB"). Essa legislação estabelece os critérios para determinar qual ordenamento jurídico regerá as relações, buscando equilibrar o respeito à soberania nacional com a necessidade de efetividade das normas estrangeiras. Dessa forma, o estudo da legislação brasileira à luz dos princípios do direito internacional — e em relação com a GDPR europeia — é imprescindível para compreender as possíveis soluções jurídicas aos conflitos decorrentes da utilização indevida de dados pessoais de titulares brasileiros por operadores situados na União Europeia.

### 3.1.1 LINDB

A LINDB (Decreto-Lei nº 4.657/1942) é um importante instrumento normativo que orienta a aplicação e a integração das leis no ordenamento jurídico brasileiro. Embora não trate diretamente da proteção de dados pessoais, a LINDB possui papel fundamental na

determinação da legislação aplicável e na solução de conflitos de leis no espaço, especialmente em casos que envolvem relações jurídicas com elementos internacionais.

Diante do crescente intercâmbio de informações e da globalização das atividades econômicas, a LINDB se torna essencial para compreender a interação do direito brasileiro com situações em que há envolvimento de normas estrangeiras, como as que regem o tratamento de dados pessoais na União Europeia.

O artigo 9º da LINDB dispõe que "*para qualificar e reger as obrigações, aplicar-se-á a lei do país em que se constituírem*" (BRASIL, 1942). Esse princípio serve de base para a solução de conflitos internacionais envolvendo contratos e responsabilidades civis. Assim, em um cenário de transferência internacional de dados, a norma orienta que a legislação aplicável deve ser aquela do local em que o vínculo jurídico foi estabelecido — o que, em muitos casos, dependerá da análise da relação entre controlador e operador.

Por exemplo, se o contrato que regula o tratamento de dados é celebrado no Brasil, e o controlador se encontra em território nacional, aplica-se, em regra, a legislação brasileira, ainda que o operador atue em país estrangeiro. Essa lógica visa assegurar previsibilidade e segurança jurídica às partes, permitindo a harmonização entre diferentes sistemas normativos.

Por outro lado, caso seja, por meio do contrato de cláusulas-tipo celebrado entre as parte, fixado como jurisdição e foro aplicável o de algum país na União Europeia, pode-se ter que a LINDB fundamentará a aplicação da lei daquele país, em detrimento do local em que foi estabelecido o vínculo jurídico.

Essa via de mão dupla da aplicação da lei, à luz do local em que foi celebrado o ato jurídico, está em plena harmonia com o quanto disposto através da Resolução CD/ANPD nº 19, por meio da qual estão dispostas as opções de escolha entre cláusulas-padrão contratuais e equivalentes.

Além disso, a LINDB reforça princípios como o da cooperação e da boa-fé nas relações jurídicas internacionais, determinando que a aplicação do direito estrangeiro não pode violar a soberania nacional, a ordem pública ou os bons costumes. Esses parâmetros são especialmente relevantes em casos que envolvem o tratamento transnacional de dados, uma vez que a proteção à privacidade e à autodeterminação informativa são consideradas expressões diretas dos direitos fundamentais assegurados pela Constituição Federal.

Dessa forma, a LINDB funciona como um elo entre o direito internacional privado e o direito constitucional brasileiro.

Com base nessas diretrizes, a LINDB atua como ponto de partida para a análise da legislação brasileira sobre proteção de dados pessoais, especialmente no contexto de conflitos normativos com a União Europeia. É a partir dessa estrutura de direito internacional privado que se torna possível compreender a aplicação e os limites da LGPD, a qual, além de regulamentar o tratamento de dados em território nacional, também disciplina as hipóteses de transferência internacional de dados e os critérios para a cooperação com outros países.

### 3.1.2 LGPD

A LGDP (Lei nº 13.709, de 14 de agosto de 2018) foi um marco importante para o desenvolvimento jurídico nacional. Logo após a edição do Marco Civil da Internet ("MCI"), em 2014, o qual desempenhou um importante papel na defesa de direitos de usuários da internet, foi confeccionada a LGDP, por meio da qual o legislador se preocupou em dar mais ênfase à proteção dos dados de todos aqueles que, de alguma forma, utilizavam a internet.

O grande papel da LGDP foi trazer segurança jurídica a todas as partes no processo de tratamento de dados, o qual, conforme visto, é composto por três agentes, quais sejam, o controlador, o operador e o titular dos dados.

Logo no artigo 1º da Lei, está disposto que a legislação seria aplicável ao tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2018).

Outro ponto importante abordado logo no início da legislação é a proteção de dados com fundamento no desenvolvimento econômico e tecnológico e na inovação, bem como na livre iniciativa, na livre concorrência e na defesa do consumidor.

Evidentemente, a LGDP se mostra como uma legislação rígida o suficiente para proteger o tratamento de dados daqueles que fazem parte do processo, mas sem deixar de lado a necessidade do desenvolvimento econômico e da livre iniciativa. Isso é importante pois, como é o caso da transferência internacional de dados, matéria objeto do presente estudo, os titulares dos dados devem contar com segurança suficiente para o tratamento dos seus dados, mas sem que isso afete a opção do controlador e do operador em se desenvolver tecnicamente e economicamente.

Além disso, por meio do artigo 6º da LGPD, estão descritos os princípios que deverão ser tomados como norte no processo e tratamento de dados pessoais. Confira-se:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.” (BRASIL, 2018)

Em que pese a importância de todos os princípios acima mencionados, no âmbito da transferência internacional de dados, o princípio da segurança se sobressai. Isso porque, conforme visto anteriormente, a transferência de dados entre países sempre será pautada na segurança que cada uma das partes poderá ofertar às outras.

Não por outro motivo, por meio da GDPR, a União Europeia elencou três maneiras diferentes de se realizar a transferência de dados para países fora da região, sendo que o mais recomendado e mais ágil é por meio da decisão de adequação, justamente por ser aquela que garante uma maior proteção aos envolvidos.

Da mesma maneira, no Brasil, a LGPD foi editada, no que tange à proteção de dados em escala internacional, pautada na proteção garantida aos envolvidos. Isso, para além de ser algo muito benéfico aos titulares dos dados, também é um estímulo ao desenvolvimento econômico do país, uma vez que as empresas, também, poderão contar com a garantia da segurança quando for realizada a transferência internacional de dados.

Para garantir a total segurança entre os envolvidos, o legislador dedicou um capítulo inteiro à transferência internacional de dados, o qual será mais bem explorado no presente estudo, a fim de comparar as suas disposições com aquelas já vistas anteriormente referente à GDPR e, por fim, concluir qual a legislação adequada para a solução de conflitos entre países da União Europeia e o Brasil.

#### 3.1.2.1 Requisitos aplicáveis para a transferência internacional de dados

A LGPD em muito se baseou na GDPR, especialmente na edição dos requisitos para que ocorra a devida transferência internacional de dados entre os países. Conforme visto, a GDPR garante que essa transferência poderá ocorrer mediante três maneiras distintas, quais sejam, por meio de uma decisão de adequação, por meio de garantias adequadas ou por meio de derrogações específicas.

No Brasil não é diferente. A transferência de dados do Brasil para qualquer outro país poderá ser feita apenas em casos em que o país importador possua grau de proteção adequado (o que se assemelha à decisão de adequação), quando o país importador comprovar garantias de cumprimento dos princípios na forme de cláusulas contratuais, cláusulas-padrão, normas corporativas ou selos, certificados e códigos de conduta regularmente emitidos (o que se assemelha com as garantias adequadas), ou quando a transferência for necessária para a integridade de princípios, como o da vida e o da incolumidade física do titular ou de terceiros, ou quando for necessária para outras hipóteses específicas (esta, de certa forma, também semelhante às derrogações específicas, variando de caso a caso).

Exatamente nesse sentido, Patrícia Garrido muito bem reforça o amparo da LGPD na GDPR, especialmente na criação de um padrão internacional de proteção de dados pessoais, impondo métodos de segurança adequados às todas as partes envolvidas. Confira-se:

> "Seguindo os parâmetros lançados pelo GDPR, a adoção da lei brasileira traz a previsão – inevitável – dos fluxos transfronteiriços de dados pessoais, de maneira que os países passíveis desse tipo de transação devem oferecer a garantia da proteção dos dados pessoais em mesmo grau que a LGPD prevê.
> Isso significa que o Brasil segue o movimento europeu de padronização internacional do fluxo de dados, assim como de proteção dessas informações, de maneira a garantir que o desenvolvimento tecnológico e econômico possa continuar seu acelerado e complexo processo, sem que com isso direitos e garantias fundamentais sejam relativizados ou violados.
> O preâmbulo (5), (6), (116) e o art. 4 (23) pontuam que a proteção de dados não deve prejudicar o desenvolvimento econômico e tecnológico no contexto global, mas que a promoção da garantia de proteção aos tratamentos dos dados deve ser eficaz e real, conforme reitera o artigo 56 (1) ao destacar que a autoridade de controle tem competência de ação no tratamento de dados transfronteiriços.
> Nesse contexto, é importante pontuar que, ainda que o ambiente digital aponte-se como naturalmente internacional, a soberania das nações deve ser respeitada. A atuação dos órgãos/cortes internacionais pode ser aumentada e expandida com essa nova realidade." (GARRIDO, 2022)

Nesse contexto, é importante pontuar que, ainda que o ambiente digital se aponte como naturalmente internacional, a soberania das nações deve ser respeitada. A atuação dos órgãos/cortes internacionais pode ser aumentada e expandida com essa nova realidade.

***No primeiro caso***, para que um país seja considerado seguro suficiente para fazer parte da transferência internacional de dados, o seu nível de segurança será avaliado pela autoridade nacional competente, no caso, a ANPD, que levará em consideração o quanto disposto no artigo 34 da LGPD. Confira-se:

> "Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:
> I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;
> II - a natureza dos dados;

> III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;
> IV - a adoção de medidas de segurança previstas em regulamento;
> V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e
> VI - outras circunstâncias específicas relativas à transferência." (BRASIL, 2018)

Ao abranger todas as qualidades mencionadas, o país importador dos dados será considerado seguro para a efetivação da transferência internacional de dados. Contudo, da mesma forma que na GDPR, caso o país não atenda às especificidades acima, ele ainda poderá fazer parte da transferência internacional de dados.

Destaque-se que, até meados de 2025, época em que o presente estudo foi realizado, ainda não há decisão de adequação emitida pelo Conselho Diretor da ANPD, de modo que, qualquer transferência internacional proveniente do Brasil deverá partir das demais soluções apresentadas pela LGPD.

Diante disso, passa-se para a ***segunda alternativa***, por meio da qual o controlador deverá oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados, por meio de (i) cláusulas contratuais específicas para determinada transferência, (ii) cláusulas-padrão contratuais, (iii) normas corporativas globais ou (iv) selos, certificados e códigos de conduta regularmente emitidos.

Nesse ponto, vale uma especial atenção às cláusulas-padrão contratuais, as quais em muito se assemelham às cláusulas-tipo da GDPR. Por meio delas, as partes celebram um acordo, pré-aprovado pela agência reguladora, que garante a existência de segurança mínima para que se desenvolva e opere a transferência internacional dos dados, sem que sejam comprometidas as partes ou os seus direitos.

Para casos em que não sejam aplicáveis as duas opções acima elencadas, não obstante a recém-editada Resolução CD/ANPD nº 19/2024, a qual ampliou e simplificou a utilização da segunda opção e que será explorada em tópico específico, a transferência internacional de dados ainda poderá ser pautada em uma terceira opção.

***Nessa terceira alternativa***, os casos são mais específicos, variando a maneira de aplicação para cada uma das hipóteses. Para isso, o legislador previu diferentes cenários em que a transferência internacional de dados poderá ocorrer, partindo de casos em que estão sendo tutelados direitos básicos da pessoa, até casos em que o titular dos dados dê ciência e consentimento expresso do tratamento dos seus dados. Confira-se:

> “Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
> (...)
> III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
> IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> V - quando a autoridade nacional autorizar a transferência;
> VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
> VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
> VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou
> IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.” (BRASIL, 2018)

Assim, o ente interessado na transferência internacional de dados contará com três opções possíveis e legalmente validadas, quais sejam, por meio de decisões de adequação, por meio de garantias adequadas, ou por meio de condições específicas para cada caso.

Evidentemente, na falta de país que seja elencado como seguro para a transferência internacional de dados por meio de uma decisão de adequação, a via mais adequada e rápida eleita para a transferência internacional de dados, atualmente, é por meio das garantias adequadas.

Recentemente, a ANPD proferiu a Resolução CD/ANPD nº 19/2024, por meio da qual foram estabelecidos os procedimentos e regras aplicáveis para a transferência internacional de dados, em conformidade com as disposições da LGPD, do Regimento Interno da ANPD e da Inciativa 4 da Agenda Regulatória para o biênio 2023-2024.

Nesse contexto, torna-se essencial compreender o papel normativo da ANPD na regulamentação e operacionalização dessas transferências. A edição da Resolução CD/ANPD nº 19/2024 representa um marco nesse processo, pois detalha os procedimentos

e critérios que devem ser observados pelas organizações interessadas, simplificando e aprimorando a aplicação prática das garantias adequadas.

## 2.2 Resolução CD/ANPD nº 19/2024

A Resolução CD/ANPD nº 19, de 23 de agosto de 2024 (ou, simplesmente, "Resolução") (BRASIL, 2024), foi um passo importante para o desenvolvimento do procedimento e das normas aplicáveis à transferência internacional de dados.

Por meio da referida Resolução, o Conselho Diretor da ANPD aprovou o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais, estabelecidas por meio da LGPD. Além disso, por meio da Resolução CD/ANPD nº 19, de 23 de agosto de 2024, foi estabelecido, pela primeira vez, o instituto das cláusulas-padrão contratuais equivalentes.

Iniciando pelas cláusulas-padrão contratuais, a Resolução CD/ANPD nº 19 prevê que as referidas cláusulas visam garantir a adoção das salvaguardas adequadas para o cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD.

Além disso, foi estabelecido o Anexo II à Resolução, por meio do qual foi editado um contrato, pré-aprovado, que possui validade para a transferência internacional de dados, que deverá ser firmado entre o exportador e o importador.

Quanto a esse ponto, em que pese a LGPD prever que apenas o controlador/importador poderá realizar a transferência internacional de dados via cláusulas-padrão contratuais, o Anexo II da Resolução prevê que, tanto o controlador quanto o operador, poderão ser considerados como importador e exportador, e vice-versa. Em outras palavras, as cláusulas-padrão contratuais serão reconhecidas em casos em que o controlador está no Brasil e exporta os dados para o operador estrangeiro, como também em casos em que o operador está no Brasil e o controlador é estrangeiro.

Portanto, para todos os fins, as cláusulas-padrão contratuais serão válidas para todos os tipos de transferência internacional de dados, independentemente de quem for o ente importador e o exportador.

Dessa maneira, caso o controlador brasileiro exporte os dados para o operador estrangeiro, como no caso da pergunta que norteia a presente pesquisa, as partes poderão optar pela utilização das cláusulas-padrão contratuais validadas pela ANPD, por meio do Anexo II da Resolução.

Uma vez superado este ponto, pode-se, livremente, analisar o quanto disposto no modelo aprovado, o qual será pactuado entre o exportador e o importador.

A cláusula 7ª do Anexo II da Resolução CD/ANPD nº 19 prevê qual será a legislação aplicável para a transferência internacional de dados, a qual será a brasileira. Confira-se:

> "CLÁUSULA 7. Legislação aplicável e fiscalização da ANPD
> 7.1. A Transferência Internacional de Dados objeto das presentes Cláusulas submete-se à Legislação Nacional e à fiscalização da ANPD, incluindo o poder de aplicar medidas preventivas e sanções administrativas a ambas as Partes, conforme o caso, bem como o de limitar, suspender ou proibir as transferências internacionais decorrentes destas Cláusulas ou de um Contrato Coligado." (BRASIL, 2024)

Evidentemente, ao celebrarem o contrato de cláusulas-padrão para a transferência internacional de dados, as partes declaram e concordam que a legislação aplicável será a brasileira.

A corroborar, por meio da cláusula 24 do contrato-padrão aprovado pela ANPD, foi fixado o foro e jurisdição para a resolução de qualquer controvérsia decorrente das cláusulas, as quais deverão ser resolvidas perante os tribunais do Brasil. A mesma disposição também valerá para controversas levadas à resolução mediante arbitragem. Confira-se:

> "CLÁUSULA 24. Eleição do foro e jurisdição
> 24.1. Aplica-se a estas Cláusulas a legislação brasileira e qualquer controvérsia entre as Partes decorrente destas Cláusulas será resolvida perante os tribunais competentes do Brasil, observado, se for o caso, o foro eleito pelas Partes na Seção IV.
> 24.2. Os Titulares podem ajuizar ações judiciais contra o Exportador ou o Importador, conforme sua escolha, perante os tribunais competentes no Brasil, inclusive naqueles localizados no local de sua residência.
> 24.3. Em comum acordo, as Partes poderão se valer da arbitragem para resolver os conflitos decorrentes destas Cláusulas, desde que realizada no Brasil e conforme as disposições da Lei de Arbitragem." (BRASIL, 2024)

Portanto, ao celebrarem o contrato de cláusulas-padrão aprovado pela ANPD, a legislação aplicável ao caso será a brasileira, bem como o foro será aquele situado no país.

Contudo, a Resolução também dispõe a respeito das cláusulas-padrão equivalentes, as quais se referem a cláusulas-padrão contratuais aprovadas por países estrangeiros ou

organismos internacionais e que podem ser reconhecidas pelas ANPD como equivalentes às cláusulas-padrão contratuais brasileiras. Uma vez consideradas como equivalentes, as partes do tratamento internacional de dados poderão utilizar essas cláusulas em suas transferências, sem a necessidade de adotar o modelo previsto no Anexo II da Resolução.

Para isso, a equivalência deverá se dar por decisão do Conselho Diretor, de ofício ou a requerimento dos interessados, será instruído por área técnica e, após manifestação da Procuradoria Federal Especializada, será objeto de deliberação pelo Conselho Diretor.

Após a sua aprovação, as partes poderão, por exemplo, celebrar um acordo de cláusulas-tipo, previsto por meio da GDPR, e que será considerado válido como cláusulas-padrão contratuais. Isso significa que, se as partes optarem por legislação e foro europeu para a resolução de demandas, por meio de cláusulas-tipo contratuais validadas nos termos do artigo 18 da Resolução, o foro aplicável será o europeu, e não mais o brasileiro.

Assim, a Resolução CD/ANPD nº 19/2024 se consolidou como um importante marco regulatório no contexto da transferência internacional de dados pessoais no Brasil, ao detalhar os instrumentos e procedimentos necessários para garantir a conformidade com os princípios da LGPD.

A criação e aprovação das cláusulas-padrão contratuais pela ANPD conferiram maior previsibilidade e segurança jurídica à transferência internacional de dados, além de ampliar a autonomia das partes ao permitir que tanto controladores quanto operadores possam figurar como exportadores ou importadores.

Ao mesmo tempo, a Resolução deixou a critério das partes a eleição do foro e jurisdição aplicável aos diferentes casos, sendo a aplicação da lei brasileira como regra para casos em que forem celebradas cláusulas-padrão contratuais nos termos do Anexo II, e podendo ser escolhida outra jurisdição para casos em que haja a celebração de contrato que seja classificado como de cláusulas-padrão equivalentes.

## CONCLUSÕES

A presente pesquisa demonstrou que a crescente digitalização das relações sociais e comerciais impõe desafios significativos à proteção de dados pessoais, especialmente quando esses dados transitam entre diferentes jurisdições. A transferência internacional de dados, embora essencial para o funcionamento de serviços globais, exige um arcabouço jurídico robusto que garanta a segurança dos titulares e a previsibilidade das relações contratuais.

A análise comparativa entre a LGPD brasileira e o GDPR europeu revelou que, embora ambas as legislações compartilhem princípios fundamentais, como a proteção da privacidade e a autodeterminação informativa, existem diferenças relevantes quanto à forma de aplicação e à definição da legislação competente em casos internacionais.

A GDPR, por exemplo, estabelece uma hierarquia clara entre decisão de adequação, garantias adequadas e derrogações específicas, enquanto a LGPD adota estrutura semelhante, mas ainda em fase de consolidação prática.

No contexto específico da transferência de dados entre operadores situados na União Europeia e controladores brasileiros, a legislação brasileira tem se mostrado cada vez mais clara e eficaz. A edição da Resolução CD/ANPD nº 19/2024 foi um marco nesse sentido, ao estabelecer cláusulas-padrão contratuais que definem expressamente a legislação brasileira como aplicável, além de prever a jurisdição nacional para resolução de conflitos.

A cláusula 7ª do Anexo II da referida Resolução é especialmente relevante, pois determina que a transferência internacional de dados estará sujeita à legislação nacional e à fiscalização da ANPD. Isso significa que, mesmo em relações contratuais com agentes estrangeiros, o Brasil assegura a aplicação de sua legislação, reforçando a proteção dos titulares nacionais e a soberania jurídica do país.

Além disso, a cláusula 24 do mesmo Anexo estabelece que qualquer controvérsia decorrente das cláusulas será resolvida perante os tribunais brasileiros, podendo, inclusive, ser submetida à arbitragem no Brasil. Essa previsão garante maior segurança jurídica aos titulares e aos agentes de tratamento situados no país, ao delimitar claramente o foro competente.

A possibilidade de reconhecimento de cláusulas-padrão equivalentes, previstas por legislações estrangeiras como o GDPR, também foi abordada pela Resolução. Essa abertura demonstra a disposição do Brasil em dialogar com outros sistemas jurídicos, desde que

respeitados os princípios e garantias previstos na LGPD. Trata-se de um avanço importante rumo à harmonização internacional das normas de proteção de dados.

A pesquisa também evidenciou que, embora o Brasil ainda não tenha sido reconhecido pela Comissão Europeia como país com nível de proteção adequado, isso não impede a realização de transferências internacionais de dados. Pelo contrário, a LGPD e a Resolução CD/ANPD nº 19 oferecem mecanismos suficientes para garantir a legalidade e a segurança dessas operações, desde que observadas as garantias adequadas.

Dessa forma, conclui-se que, nos casos envolvendo a utilização indevida de dados pessoais de titulares brasileiros por operadores situados na União Europeia, por meio de cláusulas-padrão contratuais celebradas por controlador situado no Brasil, a legislação aplicável será a brasileira. Essa escolha, contudo, não será exclusiva, podendo as partes optarem por outras legislações, desde que sejam consideradas como cláusulas-padrão equivalentes.

Por fim, o estudo reforça a importância da constante atualização e aprimoramento das normas nacionais, bem como da cooperação internacional entre autoridades reguladoras. A proteção de dados pessoais é um direito fundamental que transcende fronteiras, exigindo esforços conjuntos para garantir sua efetividade em um mundo cada vez mais interconectado.

## BIBLIOGRAFIAS


ALEMANHA. **Grundgesetz für die Bundesrepublik Deutschland** [Lei Fundamental da República Federal da Alemanha]. Bonn, 1949. Disponível em: https://www.gesetze-im-internet.de/gg/BJNR000010949.html. Acesso em: 7 set. 2025.

ALEMANHA. **Hessisches Datenschutz- und Informationsfreiheitsgesetz** (HDSIG). Lei estadual de proteção de dados e liberdade de informação do estado de Hessen, originalmente promulgada em 13 out. 1970. Última atualização em 15 nov. 2021. Disponível em: https://dsgvo-gesetz.de/hdsig/. Acesso em: 7 set. 2025.

BRASIL. **Autoridade Nacional de Proteção de Dados. 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. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-19-de-23-de-agosto-de-2024. Acesso em: 5 out. 2025.

BRASIL. **Decreto-Lei nº 4.657, de 4 de setembro de 1942. Lei de Introdução às normas do Direito Brasileiro**. Diário Oficial da União: seção 1, p. 11937, 5 set. 1942. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del4657.htm. Acesso em: 4 out. 2025.
BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016**. General Data Protection Regulation. Official Journal of the European Union, L119, p. 1–88, 2016.

GARRIDO, **Patricia P. Proteção de Dados Pessoais: Comentários À Lei N 13709/2018 (Lgpd)** - 4ª Edição 2022. 4. ed. Rio de Janeiro: Saraiva Jur, 2023. E-book. p.154. ISBN 9786555599480. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786555599480/. Acesso em: 05 out. 2025.

SILVA, Louise S. H. Thomaz da; SOUTO, Fernanda R.; OLIVEIRA, Karoline F.; et al. **Direito Digital**. Porto Alegre: SAGAH, 2021. E-book. p.96. ISBN 9786556902814. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786556902814/. Acesso em: 10 set. 2025.

SILVA, Matheus Passos. **Os desafios para a proteção de dados no contexto de transferências internacionais de dados pessoais no setor privado**. In: FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antonio (Orgs.). A Lei Geral de Proteção de Dados Pessoais: aspectos práticos e teóricos relevantes no setor público e privado. São Paulo: Thomson Reuters Brasil, 2021. p. 781.

UNIÃO EUROPEIA. **Decisão de Execução (UE) 2021/914 da Comissão, de 4 de junho de 2021**, relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Jornal Oficial da União Europeia, L 199, p. 31–61, 7 jun. 2021. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32021D0914. Acesso em: 4 out. 2025.

UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995**. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial n.º L 281 de 23/11/1995.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, L 119, p. 1–88, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 28 set. 2025.

VIGLIAR, José Marcelo M. **LGPD e a Proteção de Dados Pessoais na Sociedade em Rede**. São Paulo: Grupo Almedina, 2022. E-book. p.72. ISBN 9786556276373. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786556276373/. Acesso em: 07 set. 2025.