UNIVERSIDADE DE BRASÍLIA

Faculdade de Direito

Programa de Pós-Graduação em Direito

LUIZA MENDONÇA DA SILVA BELO SANTOS

INTEROPERABILIDADE EM TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PESSOAIS

UMA ANÁLISE CRÍTICA DOS REGIMES JURÍDICOS DE PROTEÇÃO DE DADOS DO BRASIL, ARGENTINA, URUGUAI E COLÔMBIA

Brasília

2023

UNIVERSIDADE DE BRASÍLIA

Faculdade de Direito

Programa de Pós-Graduação em Direito

LUIZA MENDONÇA DA SILVA BELO SANTOS

INTEROPERABILIDADE EM TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PESSOAIS

UMA ANÁLISE CRÍTICA DOS REGIMES JURÍDICOS DE PROTEÇÃO DE DADOS DO BRASIL, ARGENTINA, URUGUAI E COLÔMBIA

Dissertação apresentada à Banca Examinadora da Faculdade de Direito da Universidade de Brasília como requisito parcial para a obtenção do título de Mestre em Direito, elaborada sob a orientação da Prof.º Dr. Alexandre Kehrig Veronese Aguiar.

Brasília

2023

UNIVERSIDADE DE BRASÍLIA

Faculdade de Direito

Programa de Pós-Graduação em Direito

Dissertação apresentada à Banca Examinadora da Faculdade de Direito da Universidade de Brasília como requisito parcial para a obtenção do título de Mestre em Direito.

Luiza Mendonça da Silva Belo Santos

BANCA EXAMINADORA

_____

Professor Doutor Alexandre Kehrig Veronese Aguiar (Orientador)

Universidade de Brasília

_____

Professora Doutora Ana Frazão

Universidade de Brasília

_____

Doutor Thiago Luís Santos Sombra

Advogado

_____

Professor Doutor Marcio Iorio Aranha (Suplente)

Universidade de Brasília

Brasília, 20 de Dezembro de 2023

AGRADECIMENTOS

Em um ano marcado por significativos desafios pessoais, a conclusão desta pesquisa assume uma importância ainda mais especial. Minha profunda gratidão é dirigida à minha mãe, cuja força inabalável e estímulo foram a minha fonte de motivação. Seu amor incondicional inspirou a construção de cada fase deste trabalho. Este agradecimento estende-se também à minha família pelo suporte e carinho que me ofereceram ao longo da jornada.

Da mesma forma, expresso meu agradecimento ao meu orientador. A sua competência, atenção e orientação foram valiosas para este trabalho, reforçando a minha admiração por sua dedicação à educação e à pesquisa.

Além disso, é importante mencionar a Fundação de Amparo à Pesquisa do Estado de São Paulo pelo período que me concedeu a bolsa de pesquisa para o projeto "Pesquisa documental e de campo sobre autoridades de proteção de dados na América Latina: o conceito social e institucional de privacidade e de dados pessoais". Agradeço, igualmente, ao grupo de pesquisadores que compartilhou o referido projeto. A oportunidade de me aprofundar no projeto despertou meu interesse acadêmico para este trabalho.

Aos meus colegas da advocacia, agradeço pelas trocas diárias que tanto contribuíram para o amadurecimento das minhas reflexões. Por fim, agradeço ao meu namorado e aos meus amigos pelo apoio e paciência que foram fundamentais para manter o equilíbrio e a persistência durante os momentos mais intensos deste trabalho.

RESUMO

No decorrer do tempo, as transferências internacionais de dados deixaram de ser eventos pontuais e transformaram-se em operações regulares na realidade cotidiana de entidades públicas e privadas. Esta pesquisa concentra-se na avaliação do fenômeno na perspectiva regulatória de proteção de dados. Nesse particular, dois desafios têm ocupado posição central nas discussões, quais sejam, a diversidade de leis nacionais para a proteção de dados e privacidade ao redor do mundo, que podem disciplinar níveis variados de proteção, e a prática de entidades transferirem dados pessoais para países com padrões de proteção menos rigorosos. Nessa direção, as leis de proteção de dados têm buscado estabelecer regimes para a tutela das transferências internacionais de dados pessoais, de modo a manter a continuidade da proteção conferida aos dados pessoais ao cruzarem as fronteiras. Na América Latina, a trajetória de proteção de dados está avançando. Diante desse panorama, esta pesquisa se propõe a buscar a resposta para a seguinte pergunta: de que maneira as leis de proteção de dados do Brasil, da Argentina, do Uruguai e da Colômbia estruturaram os seus regimes de transferências internacionais de dados pessoais e qual é o impacto desses regimes para a promoção das transferências nessa região? A busca por mecanismos e procedimentos interoperáveis é importante para assegurar fluxos de dados seguros e confiáveis entre os países. Desse modo, esta pesquisa se insere na área de concentração de "Direito, Estado e Constituição", do Programa de Pós-Graduação em Direito da Universidade de Brasília, aderindo à linha de pesquisa de "Transformações na Ordem Social e Econômica e Regulação", com enfoque na sublinha de pesquisa de "Regulação Social e Políticas Públicas de Educação, Ciência, Tecnologia e Inovação". Da mesma forma, ela está relacionada ao projeto "Pesquisa documental e de campo sobre autoridades de proteção de dados na América Latina: o conceito social e institucional de privacidade e de dados pessoais" da Universidade de Brasília, que contou com o apoio da Fundação de Amparo à Pesquisa do Estado de São Paulo. Para tanto, será abordado o papel da Internet e das tecnologias de informação e comunicação na evolução das transferências internacionais de dados pessoais, discutindo as contribuições das teorias de regulação da Internet para a avaliação de abordagens regulatórias híbridas, bem como examinando instrumentos internacionais e regionais relevantes. Em seguida, será analisado o modelo regulatório de proteção de dados da União Europeia, sua influência da região latino-americana e o seu contraste com o modelo dos Estados Unidos da América. Com isso, serão avaliados os regimes de tutela das transferências internacionais de dados pessoais específicos de cada país objeto da análise e, depois, em perspectiva comparada. Por fim, conclui-se que mecanismos voluntários, como instrumentos contratuais e normas corporativas vinculantes ou globais, configuram-se meios para promover os fluxos de dados entre os países, exigindo dos agentes envolvidos práticas responsáveis, prestação de contas e análises dos riscos associados às transferências. Ressalta-se a importância de se estabelecer balizas para a proteção integral dos dados, inclusive em contextos de atividades de segurança e persecução penal, e de que os países considerem essa pauta.

Palavras-chave: Proteção de Dados; Transferências Internacionais de Dados Pessoais na América Latina.

ABSTRACT

Over time, international data transfers have evolved from sporadic events to regular operations in the daily reality of both public and private entities. This research focuses on evaluating this phenomenon from a data protection regulatory perspective. More specifically, two key challenges have emerged as focal points in debates: the diversity of national laws for data protection and privacy around the world, which may prescribe varying levels of protection, and the practice of entities transferring personal data to countries with less stringent protection standards. In this regard, data protection laws have sought to establish regimes for governing international personal data transfers, aiming to maintain the continuity of protection afforded to personal data as they cross borders. In Latin America, the development of data protection is advancing. Given this scenario, this research aims to answer the following question: How have the data protection laws of Brazil, Argentina, Uruguay, and Colombia structured their regimes for international personal data transfers, and what is the impact of these regimes on promoting transfers in this region? The pursuit of interoperable mechanisms and procedures is important for ensuring safe and reliable data flows between countries. In this context, this research situates itself within the "Law, State, and Constitution" area of focus, part of the Postgraduate Program in Law at the University of Brasília. It adheres to the research area of "Transformations in the Social and Economic Order and Regulation", placing particular emphasis on the research sub-area of "Social Regulation and Public Policies in Education, Science, Technology, and Innovation". Concurrently, this study is linked to the project "Documentary and field research on data protection authorities in Latin America: the social and institutional concept of privacy and personal data" of the University of Brasília, which was supported by the São Paulo Research Foundation. This research will explore the role of the Internet and information and communication technologies in the evolution of international personal data transfers, discussing the contributions of Internet regulation theories to the assessment of hybrid regulatory approaches, as well as examining relevant international and regional instruments. Subsequently, the European Union's data protection regulatory model, its influence in the Latin American region, and its contrast with the United States model will be analyzed. As a result, the regimes governing international transfers of personal data specific of each country under analysis will be evaluated, followed by a comparative perspective assessment. The research concludes that voluntary mechanisms, such as contractual instruments and binding corporate or global rules, are means to promote data flows between countries, requiring responsible and accountable practices, and risk analysis associated with the transfers from the involved parties. Finally, the importance to define parameters for comprehensive data protection is highlighted, including in contexts of security activities and criminal prosecution, and the need for countries to consider this agenda.

Keywords: Data Protection; International Transfers of Personal Data in Latin America.

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AAIP	*Agencia de Acceso a La Información Publica*
AGESIC	*Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento*
ANPD	Autoridade Nacional de Proteção de Dados
APD	Autoridades de Proteção de Dados
APEC	Cooperação Econômica Ásia-Pacífico
CBPR	*Cross-Border Privacy Rules*
DNPDP	*Dirección Nacional de Protección de Datos Personales*
EIPD	Encontro Ibero-americano de Proteção de Dados
EUA	Estados Unidos da América
FISA	*Foreign Intelligence Surveillance Act*
FTC	*Federal Trade Commission*
IDPC	*Irish Data Protection Commission*
LED	*Law Enforcement Directive*
LGPD	Lei Geral de Proteção de Dados
LOPD	*Ley Orgánica de Protección de Datos*
LORTAD	*Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal*
MERCOSUL	Mercado Comum do Sul
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
PRP	*Privacy Recognition for Processors*
RGPD	Regulamento Geral sobre a Proteção de Dados
RIPD	Rede Ibero-americana de Proteção de Dados
SIC	*Superintendencia de Industria y Comercio*
STF	Supremo Tribunal Federal
TIC	Tecnologias de Informação e Comunicação
TJUE	Tribunal de Justiça da União Europeia
UE	União Europeia
URCDP	*Unidad Reguladora y de Control de Datos Personales*

SUMÁRIO

INTRODUÇÃO

Considere o cenário hipotético de uma empresa estabelecida no Brasil, a "AlphaTech", que oferece uma plataforma de comércio eletrônico e coleta dados pessoais de seus usuários para fornecer seus serviços, como dados cadastrais, dados de pagamento, dados de localização, entre outros. Nesse processo, a "AlphaTech" armazena os dados coletados em servidores da empresa "DataNuvem", localizados na Uruguai. Paralelamente, na Argentina, a "BetaInova", que integra o grupo econômico da "GamaInova" na Colômbia, rotineiramente envia dados pessoais de seus funcionários para o banco de dados de recursos humanos, centralizado na Colômbia. Em outro cenário, os governos do Brasil e da Argentina desejam criar um sistema integrado para monitorar a propagação de doenças infecciosas em regiões de fronteira. Para tanto, dados relacionados à saúde de seus cidadãos devem ser transmitidos entre os dois países. Embora sejam fictícios, os cenários ilustram o fenômeno que será tratado ao longo desta pesquisa: as transferências internacionais de dados na região da América Latina.

No decorrer do tempo, as transferências de dados entre países deixaram de ser eventos pontuais e transformaram-se em operações regulares e quase instantâneas na realidade cotidiana de entidades públicas e privadas. A globalização dos negócios pode exigir a distribuição de dados entre entidades empresariais em diferentes localidades para otimizar processos.[1] Além disso, empresas de todos os portes têm buscado benefícios econômicos e recursos de armazenamento e processamento de dados em regiões distintas do globo. As transferências também podem ser movidas por estratégias de segurança e para a recuperação de desastres, com o intuito de garantir que os dados estejam seguros e acessíveis. Ainda, as empresas podem ser obrigadas a transferir dados para cumprir requisitos contratuais. Os Estados, por sua vez, são motivados a transferir dados para o desenvolvimento de políticas públicas e pesquisas, investigação e persecução de crimes, entre outras situações. Assim, não é exagero afirmar que as transferências internacionais de dados constituem as bases para atividades essenciais na atualidade.

Embora essa situação possa impactar diversas áreas do Direito, esta pesquisa concentra-se na perspectiva regulatória de proteção de dados. Nesse particular, dois desafios têm ocupado posição central nas discussões e servem como ponto de partida para

---

[1] OCDE. Moving forward on data free flow with trust**: new evidence and analysis of business experiences**. OECD Digital Economy Papers, n. 353. Paris, OCDE, 2023. Disponível em: https://www.oecd-ilibrary.org/science-and-technology/moving-forward-on-data-free-flow-with-trust_1afab147-en. Acesso em: 2 nov. 2023.

esta pesquisa.[2] O primeiro refere-se à diversidade de leis nacionais voltadas à proteção de dados e da privacidade ao redor do mundo, que podem disciplinar níveis variados de proteção. De acordo com o levantamento conduzido por Graham Greenleaf em 2023, há, pelo menos, 162 países que introduziram textos legais nessa matéria.[3] Outra característica é a instituição de autoridades administrativas de proteção de dados (APD) para a aplicação das leis. O segundo emerge quando entidades exploram tais variações, transferindo dados pessoais para países com padrões de proteção menos rígidos, com o intuito de contornar as leis nacionais. Nessa direção, as leis de proteção de dados têm buscado estabelecer regimes para a tutela das transferências internacionais, de modo a manter a continuidade da proteção conferida aos dados pessoais ao cruzarem as fronteiras.

Na América Latina, a trajetória de proteção de dados está em evolução. Na virada do milênio, por exemplo, a Argentina aprovou a Lei nº 25.326, sendo a *Agencia de Acceso a La Información Publica* (AAIP) hoje responsável pela sua aplicação.[4] Em uma progressão similar, o Uruguai, em 2008, implementou a Lei nº 18.331, atribuindo a supervisão da norma à *Unidad Reguladora y de Control de Datos Personales* (URCDP).[5] Avançando para 2012, a Colômbia promulgou a Lei nº 1.581, com a *Superintendencia de Industria y Comercio* (SIC) atuando como autoridade reguladora.[6] No Brasil, a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, foi sancionada em 2018, criando a Autoridade Nacional de Proteção de Dados (ANPD) como a entidade responsável.[7] Cada uma dessas leis estabeleceu regimes para disciplinar a tutela das transferências internacionais de dados pessoais.

---

2 KUNER, Christopher. Regulation of transborder data flows under data protection and privacy law: past, present, and future. **TILT Law & Technology**, Working Paper, n. 016, 10 out. 2010. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1689483. Acesso em: 2 nov. 2023.

3 GREENLEAF, Graham. Global data privacy laws 2023: 162 national laws and 20 Bills. **181 Privacy Laws and Business International Report (PLBIR),** 1, 2-4, 6 fev. 2023. Disponível em: https://www.privacylaws.com/reports-gateway/articles/int181/int181_2023/. Acesso em: 2 nov. 2023.

4 ARGENTINA. Lei nº 25.326, de 30 de outubro de 2000. Ley de Protección de Datos Personales. **Boletín Oficial:** Buenos Aires, ano 2000, n. 29517, p. p. 2 nov. 2000. p. 1. Disponível em: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/actualizacion. Acesso em: Acesso em: 2 nov. 2023.

5 URUGUAI. Ley nº 18.331 de 2008. Ley de Protección de Datos Personales. **Registro Nacional de Leyes y Decretos**, Motevidéo, ano 2008, tomo 1, semestre 2, p. p. 18 ago. 2008. p. 378. Disponível em: https://www.impo.com.uy/bases/leyes/18331-2008. Acesso em: 2 nov. 2023.

6 COLOMBIA. Ley Estatutaria nº 1.581 de 17 de outubro 2012. Por la cual se dictan disposiciones generales para la protección de datos personales: **Función Pública,** ano 139, n. 8, 17 out 2012. p. 1-74,. Disponível em: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html. Acesso em: 2 nov. 2023.

7 BRASIL. Lei nº 13,709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: seção 1, Brasília, DF, ano 139, n. 8, p. p. 14 ago 2018. p. 1-74. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 2 nov. 2023.

Diante desse panorama, esta pesquisa se propõe a buscar a resposta para a seguinte pergunta: de que maneira as leis de proteção de dados do Brasil, da Argentina, do Uruguai e da Colômbia estruturaram os seus regimes de transferências internacionais de dados pessoais e qual é o impacto desses regimes para a promoção das transferências nessa região? Com isso, é possível vislumbrar, ao menos, duas hipóteses. A primeira aborda a influência do modelo regulatório de proteção de dados da União Europeia (UE) na estrutura dos regimes dos países sob análise e também envolve a discussão sobre o contraste da construção jurídica de proteção de dados dos Estados Unidos da América (EUA). A segunda sugere que, embora os regimes dos países partam de uma base comum, podem existir variações na sua implementação que afetam as transferências entre eles.

A importância de se buscar mecanismos e procedimentos interoperáveis para as transferências internacionais de dados pessoais não se restringe a um exercício puramente acadêmico, mas decorre de uma necessidade real de promover fluxos de dados seguros e confiáveis, que são fundamentais para o desenvolvimento social, econômico e tecnológico dos países abordados nesta pesquisa.[8] A interoperabilidade jurídica é descrita por Rolf H. Weber como o processo por meio do qual normas relativas a um mesmo tema em diferentes jurisdições interagem de forma compatível, especialmente no contexto das tecnologias de informação e comunicação (TIC).[9] Essa interação estimula a troca e a compreensão de informações de maneira consistente e acessível entre as diferentes jurisdições.[10] Como resultado, a interoperabilidade jurídica favorece que indivíduos desfrutem da mesma proteção de direitos dentro de diferentes sistemas jurídicos.

A seleção do Brasil, da Argentina, do Uruguai e da Colômbia, como foco deste trabalho, foi embasada pela "Pesquisa documental e de campo sobre autoridades de proteção de dados na América Latina: o conceito social e institucional de privacidade e de dados pessoais", projeto que contou com o apoio da Fundação de Amparo à Pesquisa do Estado de São Paulo e que tive a oportunidade de integrar a equipe de pesquisadores.[11] Por conseguinte, a seleção dos países objeto do presente trabalho deu-se após um

---

[8] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. São Paulo: **Revista dos Tribunais**, 2019.

[9] WEBER, Rolf H. Legal Interoperability as a Tool for Combatting Fragmentation. Global Commission on Internet Governance, **Paper Series** n. 4, dez. 2014. Disponível em: https://www.cigi*online*.org/sites/default/files/gcig_paper_no4.pdf. Acesso em: 2 nov. 2023.

[10] WEBER, 2014. p. 5.

[11] VERONESE, Alexandre, et al. Pesquisa documental e de campo sobre autoridades de proteção de dados na América Latina: **o conceito social e institucional de privacidade e de dados pessoais**. 2022, Biblioteca Virtual da FAPESP. Disponível em: https://bv.fapesp. br/en/auxilios/105576/documentary-and-field-research-on-the-latin-american-data-protection-authorities-the-social-and-inst/. Acesso em: 2 nov. 2023.

levantamento prévio na região de enunciados constitucionais, de leis de proteção de dados aprovadas, da presença e atuação das APD e da adesão dos países a instrumentos internacionais e regionais em matéria de proteção de dados. A Argentina e o Uruguai destacaram-se por serem países latino-americanos reconhecidos por uma decisão de adequação da Comissão Europeia para receber dados pessoais da UE e pela sua adesão à Convenção 108 e 108+ do Conselho da Europa, elementos relevantes para esta pesquisa. A Colômbia, com uma APD ativa e pelo seu papel de relevo na Rede Ibero-americana de Proteção de Dados, também foi uma seleção estratégica. Já o Brasil, com sua legislação de proteção de dados recentemente aprovada e em fase de desenvolvimento quanto às transferências internacionais de dados pessoais, oferece um caso interessante de análise em construção.

Ao tratar dos regimes de tutela das transferências internacionais de dados pessoais previstos nas leis de proteção de dados de países da América Latina, esta pesquisa se insere na área de concentração de "Direito, Estado e Constituição", do Programa de Pós-Graduação em Direito da Universidade de Brasília, aderindo à linha de pesquisa de "Transformações na Ordem Social e Econômica e Regulação", com enfoque na sublinha de pesquisa de "Regulação Social e Políticas Públicas de Educação, Ciência, Tecnologia e Inovação".

Ainda que a regulação de proteção de dados envolva aspectos diversos, esta pesquisa não pretende abranger todos os conceitos jurídicos que permeiam o tratamento de dados pessoais. O seu propósito se concentra nas transferências internacionais de dados e nas questões que guardam relação direta com elas. Cabe notar que a literatura jurídica apresenta termos distintos para descrever o processo pelo qual os dados pessoais são movidos de um país para outro. Expressões como "fluxo transfronteiriço de dados pessoais" e "movimento internacional de dados pessoais" podem ser encontradas. Para efeitos deste trabalho, foi adotado o termo "transferência internacional de dados pessoais", pois é a nomenclatura empregada nas leis dos países analisados.

Para abordar as questões pretendidas, optou-se por recorrer a caminhos metodológicos complementares. Conjuga-se a revisão da literatura jurídica de proteção de dados, incluindo obras produzidas por autores da América Latina, com a análise qualitativa de instrumentos internacionais e regionais em matéria de proteção de dados, das leis de proteção de dados dos países sob análise e de fontes documentais das suas respectivas APD. Nesse sentido, esta pesquisa não se restringe à entabulação das leis de

proteção de dados dos países analisados. Em vez disso, ela busca compreender a racionalidade regulatória, sua contextualização e seus efeitos práticos.[12]

Assim, esta pesquisa está estruturada em três capítulos, além desta introdução e da conclusão. O primeiro capítulo iniciará tratando do papel dos dados pessoais, das TIC e da Internet para a evolução das transferências internacionais de dados. Discute-se a crescente relevância social, econômica e política dos dados pessoais, os novos riscos à privacidade e o desenvolvimento jurídico em torno da proteção de dados. Além disso, examina-se como as TIC e a Internet promovem a disponibilidade dos dados e a sua transposição para além das fronteiras. A partir de contribuições das teorias de regulação da Internet, será possível observar que os regimes para a tutela das transferências internacionais de dados pessoais podem alcançar maior interoperabilidade com base em abordagens regulatórias híbridas. Com base nisso, serão analisadas as iniciativas de organizações e fóruns internacionais, regionais e econômicos para a construção de padrões comuns para a conformidade jurídica relacionada às transferências internacionais de dados pessoais.

Em seguida, o segundo capítulo se debruça sobre o contraste entre os modelos regulatórios de proteção de dados da UE e dos EUA, bem como os seus impactos para as transferências transatlânticas de dados pessoais ao longo dos anos. Sob esse enfoque, será possível notar a importância da interconexão entre os diferentes sistemas jurídicos para a promoção das transferências internacionais de dados pessoais. Discute-se o movimento crescente nos EUA para a reformulação da sua construção jurídica de proteção de dados. Além disso, explora-se a evolução da proteção de dados na América Latina, aprofundando os modelos regulatórios adotadas pelo Brasil, Argentina, Uruguai e Colômbia e estabelecendo as bases para a análise dos seus regimes de tutela das transferências internacionais de dados pessoais.

No terceiro capítulo, busca-se delimitar o conceito jurídico de transferência internacional de dados pessoais a partir das leis de proteção de dados dos países abordados, diferenciando-o da coleta internacional de dados pessoais. Com isso, serão analisados os regimes de tutela das transferências internacionais de dados pessoais específicos de cada país e, depois, em perspectiva comparada, de modo a avaliar como podem impactar a promoção dos fluxos de dados entre os países. Desse modo, frente aos regimes, entende-se que mecanismos voluntários, sobretudo instrumentos contratuais e

[12] ARANHA, Mário Iório. Diálogo político-jurídico na comparação de modelos regulatórios de comunicação. **Revista Brasileira de Políticas de Comunicação**, v.1. 2011. p. 1-20.

normas corporativas vinculantes ou globais, configuram-se alterativas para promover os fluxos de dados entre os países analisados. Esses mecanismos requerem a adoção e comprovação de práticas responsáveis e de prestação de contas por parte dos agentes envolvidos, além de análises dos riscos associados às transferências.

Por fim, entende-se que a temática de transferências internacionais de dados pessoais reflete a necessidade de estabelecer balizas para a proteção integral dos dados pessoais, com atenção também para os contextos de atividades de segurança e persecução penal. Ressalta-se a importância de que os países latino-americanos considerem essa pauta em seus quadros legais de proteção de dados.

1. A EVOLUÇÃO DAS TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PESSOAIS E O SEU PANORAMA EM INSTRUMENTOS INTERNACIONAIS E REGIONAIS

1.1. Componentes-chave para a evolução das transferências internacionais de dados pessoais

Os dados pessoais, as TIC e a Internet são componentes-chave para a evolução das transferências internacionais de dados. Os dados pessoais assumiram relevância sem precedentes no âmbito social, econômico e político, tornando-se indispensáveis para diversas atividades que se estendem ao redor do mundo. Essa ascensão acarretou novos riscos relacionados à privacidade, o que, por sua vez, incentivou discussões jurídicas que resultaram no reconhecimento de um direito autônomo à proteção de dados. O aumento da relevância dos dados pessoais não teria ocorrido sem o desenvolvimento das TIC, que contribuíram para a maior disponibilidade dos dados e revolucionaram a forma como são transferidos entre os países. A Internet, igualmente, desempenha um papel central nessa dinâmica, possibilitando que os dados pessoais ultrapassem fronteiras. A análise desse cenário será objeto da primeira parte desta Seção.

Nesse contexto interconectado, surgem desafios para a regulação jurídica. A regulação estatal tradicional opera com base em fronteiras físicas, criando sistemas jurídicos que impõem obrigações dentro de áreas geográficas. Contrariamente, a Internet promoveu um ambiente virtual, no qual as atividades envolvem diferentes sistemas jurídicos e podem estar sujeitas à sobreposição de leis. Essa problemática conduz a um debate mais profundo sobre o papel do regulador,[13] o que será explorado na segunda parte desta Seção, a partir das contribuições das teorias de regulação da Internet.

1.1.1. Dados pessoais

Antes de avançar, convém definir os conceitos de "dado" e "informação". Embora muitas vezes sejam empregados indistintamente, a precisão desses conceitos é relevante no contexto regulatório. [14] Segundo Michael Buckland, o conceito de "dado" é

---

[13] REIGADA, Antonio Troncoso. El desarrollo de la protección de datos personales em Iberoamérica desde una perspectiva comparada y el reequilibro en los modelos de datos a nível internacional. **Revista Internacional de Protección de Datos Personales**, n. 1. dez. 2012. pp. 4-41. Disponível em: https://habeasdatacolombia.uniandes.edu.co/wp content/uploads/10_Antonio-troncoso_FINAL.pdf. Acesso em: 2 nov. 2023.

[14] VERONESE, Alexandre. The right of explanation and the right to object automatic decisions: **comparing the European Union General Data Protection Regulation (EU/GDPR) with the Brazilian General Data Protection Federal Act (BGDPFA)**. CPR LATAM Conference, Cordoba, Argentina, 2019. Disponível em: https://www.researchgate.net/publication/333599973_The_right_of_explanation_and_the_right_to_ob

utilizado para descrever a informação ainda não submetida a tratamento.[15] Na mesma linha, Raymond Wacks se refere ao dado como a informação em estado potencial.[16] Ao serem organizados e estruturados, dados brutos são convertidos em informação e passam a ter um significado útil.[17] Determinados dados podem ter vínculo objetivo com um indivíduo. Os dados pessoais, assim, são definidos como aqueles que podem identificar e revelar aspectos sobre o indivíduo a que se referem, denominado de titular dos dados.[18]

O crescimento da capacidade computacional possibilitou o tratamento de grandes volumes de dados pessoais para extração de informações valiosas a respeito dos seus titulares.[19] Progressivamente, os dados pessoais assumiram relevância social, econômica e política e, mais do que isso, tornaram-se grande fonte de poder que se espraia por diferentes dimensões.[20] Essa ascensão é frequentemente comparada à do petróleo, uma analogia que destaca a importância atribuída aos dados pessoais na atualidade. Assim como o petróleo é extraído, refinado e transformado em uma variedade de produtos úteis, os dados pessoais podem ser coletados, processados e utilizados para atender a diversas finalidades. Com isso, os dados pessoais passaram a ser indispensáveis para inúmeras atividades.[21]

No setor privado, os dados pessoais são considerados ativos que impulsionam os negócios.[22] Eles são parte das estratégias das empresas para otimizar suas operações, inovar e personalizar produtos e serviços. A análise de dados pessoais pode revelar padrões de consumo, preferências e comportamentos para o desenvolvimento de estratégias de publicidade, classificação de crédito e a criação de experiências

---

ject_automatic_decisions_comparing_the_European_Union_General_Data_Protection_Regulation_EUGDPR_with_the_Brazilian_General_Data_Protection_Federal_Act_BGDPF. Acesso em: 2 nov. 2023.

15 BUCKLAND, Michael. Information and information systems. Westport, CT: Praeger, 1991. p. 45.

16 WACKS, Raymond. **Personal information**. Oxford: Clarendon Press, 1989. p. 25.

17 DAVENPORT, Thomas H.; PRUSAK, Laurence. Working knowledge: How organizations manage what they know. **Harvard Business Press**, 1998. p. 63.

18 DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**, v. 12, n. 2, p. 91-108, 2011. pp. 93-94.

19 MAYER-SCHÖNBERGER, Viktor. CUKIER, Kenneth. **Big Data: como extrair volume, variedade, velocidade e valor da avalanche de informações cotidianas**. Rio de Janeiro, Elsevier. 2013. Tradução Paulo Polzonoff Junior.

20 FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 2ª ed. São Paulo: RT. 2020. pp. 23-52.

21 SRNICEK, Nick. **Platform capitalism**. Cambridge, UK; Malden, MA: Polity Press, 2017.

22 STUCKE, Maurice E. Should we be concerned about data-opolies? **Georgetown Law Technology Review**, v. 2, 2017 p. 275.

personalizadas.[23] Ainda, com a crescente utilização de redes sociais e outras plataformas digitais, houve um aumento significativo de dados pessoais disponíveis, que regularmente são fornecidos de forma voluntária pelos seus titulares. [24] No setor público, os dados pessoais podem contribuir para a formulação e implementação de políticas públicas, além de servirem como evidências para a investigação e a repressão de crimes, auxiliando na prevenção e na resposta de ameaças à segurança.

Nessa estrutura, Julie Cohen dispõe que a era atual é marcada pelo *capitalismo informacional*, [25] no qual diferentes agentes, privados e públicos, em níveis nacional e internacional, apoiam-se em dados pessoais para tomar decisões e fazer previsões. A despeito das eficiências, o uso de dados pessoais e o poder dele decorrente alteraram significativamente os riscos ao seu redor.[26] Esse panorama provocou transformações nas discussões jurídicas acerca da privacidade,[27] que passou a ser percebida não apenas como um direito negativo para assegurar o isolamento dos indivíduos, mas também como um direito positivo para permitir o controle sobre seus próprios dados.[28]

Sob essa perspectiva, os debates regulatórios passaram a reconhecer a proteção de dados pessoais como um direito autônomo que transcende a noção de privacidade. Enquanto a proteção jurídica da privacidade no âmbito internacional ganhou destaque com a introdução de compromissos de Direitos Humanos, como a Declaração Universal dos Direitos Humanos de 1948 e o Pacto Internacional sobre Direitos Civis e Políticos de 1966, a proteção de dados pessoais passou a se cristalizar com iniciativas de organizações internacionais e regionais e com a aprovação de leis nacionais sobre o tema.[29] Na atualidade, as leis de proteção de dados se espalharam pelo mundo, como é o caso do Brasil, da Argentina, do Uruguai e da Colômbia. Os regimes estabelecidos por

---

23 STIGLITZ, Joseph. **People, power, and profits: progressive capitalism for an age of discontent**. Penguin UK, 2019.

24 FRAZÃO, Ana; SANTOS, Luiza Mendonça da Silva Belo. Plataformas Digitais e o Negócio de Dados: necessário diálogo entre o Direito da Concorrência e a Regulação dos Dados. **Direito Público**, v. 17, n. 93, 2020. Disponível em: https://www.portaldeperiodicos.idp. edu.br/direitopublico/article/view/3695. Acesso em: 2 nov. 2023.

25 COHEN, Julie E. **Between truth and power: the legal constructs of information capitalism**. New York: Oxford University Press, 2019. p. 6.

26 FRAZÃO, Ana. Plataformas digitais, big data e riscos para os direitos da personalidade. In: TEPEDINO, Gustavo; MENEZES, Joyceane. **Autonomia privada, liberdade existencial e direitos fundamentais**. Belo Horizonte: Forum, 2019. pp. 333-349.

27 DONEDA, 2019.

28 RODOTÀ, Stefano. **El derecho a tener derechos**. Madrid: Trotta, 2014.

29 KUNER, 2010. p. 9.

essas leis para a tutela das transferências internacionais de dados pessoais visam assegurar que a proteção acompanhe os dados ao cruzarem as fronteiras.

Segundo Danilo Doneda, o direcionamento conferido à proteção de dados pode ser observado historicamente com base em quatro gerações regulatórias de leis de proteção de dados, que avançaram de um enfoque limitado para um mais abrangente.[30] A primeira geração de leis refletia o estado tecnológico da época e concentrava-se na autorização para a criação de bases de dados e no uso subsequente dessas bases, por entidades públicas. A segunda geração de leis surgiu no final dos anos 1970. A diferença central dessa geração em relação à anterior é a garantia de direitos aos titulares para demandar o controle de seus dados pessoais. Isso marca uma clara transição para o exercício de direitos positivos.

A terceira geração de leis, por sua vez, passou a perceber a proteção de dados como um processo complexo, ligado à participação social do titular e ao contexto em que seus dados são obtidos, oferecendo outros meios de proteção em situações nas quais os controles individuais não podem ser exercidos de forma plena. Nessa direção, a quarta geração de leis surgiu em resposta às limitações de um enfoque individual. Essas leis passaram a abordar a regulação de maneira mais abrangente, entendendo que a proteção de dados não deve se basear apenas em escolhas individuais, mas também em instrumentos que ampliem a proteção coletiva dos dados pessoais.[31-32] Tais nuances podem ser notadas na trajetória normativa dos países latino-americanos sob análise na Seção 2.3.

Diante da dimensão coletiva da proteção de dados, além dos titulares dos dados, também é importante definir os agentes responsáveis pelo tratamento desses dados, que podem variar a depender do seu grau de autonomia. Com base na literatura jurídica e nos textos legais em matéria de proteção de dados analisados, para efeitos desta pesquisa, o termo *controlador de dados* será empregado adiante para os agentes responsáveis pelas decisões relacionadas ao tratamento dos dados, e o termo *operador de dados* para os agentes que realizam o tratamento dos dados em nome do controlador. No entanto, as definições específicas previstas nas legislações de proteção de dados dos países latino-americanos abordados nesta pesquisa serão exploradas na Seção 3.1.

---

30 DONEDA, 2011. p 96.

31 DONEDA, 2011. pp. 97-98.

32 MAYER-SCÖNBERGER. General development of data protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). **Technology and privacy: The new landscape**. Cambridge: MIT Press, 1997. pp. 219-241.

O aumento da relevância dos dados pessoais nas diferentes esferas acima identificadas não teria sido possível sem o desenvolvimento das TIC, como será analisado a seguir.

1.1.2. Tecnologias de Comunicação e Informação, TIC

As TIC referem-se ao conjunto de recursos tecnológicos usados para tratar informações e promover a sua comunicação.[33] Esses recursos contribuíram para a maior disponibilidade de dados pessoais por meio da digitalização, aumento de armazenamento, processamento e conectividade, e permanecem em constante desenvolvimento.[34] A evolução das transferências internacionais de dados pessoais é frequentemente atribuída às TIC. No passado, essas transferências eram realizadas de forma ocasional e os meios para o tratamento de dados pessoais estavam, na sua maioria, circunscritos ao território nacional. Além disso, as transferências se caracterizavam por eventos estáticos, já que não ocorriam continuamente e se limitavam a um número reduzido de agentes.[35]

Em comparação ao paradigma anterior, Paul M. Schwartz observa duas mudanças significativas na forma como as transferências internacionais de dados pessoais são realizadas atualmente.[36] A primeira está relacionada ao crescimento do volume de dados transferidos. A segunda diz respeito à dinamicidade e complexidade das transferências, que agora passam por múltiplos pontos ao redor do mundo. As mudanças identificadas pelo autor possibilitaram novos negócios, incluindo a reorganização de funções e de atividades em unidades modulares, bem como alternativas adicionais para estruturar as relações internas e externas das organizações.[37]

A computação em nuvem é uma tecnologia marcante para as transformações das transferências internacionais de dados pessoais. Ela permite o acesso, normalmente via Internet, a recursos como servidores e aplicações, de forma dinâmica e escalável. Esses recursos podem ser ajustados de acordo com as necessidades dos usuários, que não mais precisam deter ou manter infraestrutura física própria. Evidências de uma pesquisa

---

33 RIGAUDIAS, Cecilia Álvarez. Personal Data Protection. In.: MARTINEZ, Aurelio López-Tarruella; MIRETE, Carmen María García (Org.). **Derecho TIC: derecho de las tecnologías de la información y de la comunicación**, 2016. pp. 363-403.

34 LLOYD, Ian J. **Information Technology Law**. Oxford: Oxford University Press, 2017.

35 SCHWARTZ, Paul M. **Managing Global Data Privacy: Cross-Border information flows in a networked environment**. Privacy Projects, 2009. Disponível em: https://paulschwartz.net/wp-content/uploads/2019/01/Global_Data_Flows.pdf. Acesso em: 2 nov. 2023.

36 SCHWARTZ, Paul M. Information privacy in the cloud. **U. Pa. L. Rev**., v. 161, p. p. 2012. pp. 1623-1662.

37 SCHWARTZ, 2012. p. 1631.

global apontada por Christopher Millard indicam que, até 2020, 90% das empresas já utilizavam ativamente recursos de computação em nuvem, enquanto os 10% restantes planejavam migrar para a nuvem.[38] A distribuição dos recursos de computação em nuvem ao redor do globo tem o potencial de mover operações entre diversos países, a partir de fatores como capacidade de carga, horário do dia, entre outros.

Enquanto as nuvens privadas são espaços dedicados a um usuário, as nuvens públicas podem ser compartilhadas e são baseadas em três modelos de serviço frequentemente utilizados hoje, quais sejam: Software como Serviço (SaaS), Plataforma como Serviço (PaaS) e Infraestrutura como Serviço (IaaS). O SaaS permite o acesso a *softwares* e aplicações na Internet através de uma interface com o usuário, como é o caso de um navegador da web. A PaaS oferece aos usuários uma plataforma integrada na Internet para o desenvolvimento e a implantação de *softwares* e aplicações. A IaaS disponibiliza recursos de infraestrutura por meio da Internet, como servidores, eliminando a necessidade de os usuários manterem equipamentos físicos.[39]

A Internet das Coisas (em inglês, *Internet of Things* ou IoT) se junta às tecnologias que impactaram a dinâmica das transferências internacionais de dados pessoais. A IoT refere-se a objetos físicos, equipados com sensores e *softwares*, que são conectados a outros dispositivos por meio da Internet, permitindo a troca de dados de forma autônoma.[40] Esses objetos podem ser controlados remotamente e variam entre *smartphones*, eletrodomésticos inteligentes, assistentes virtuais, veículos conectados, dispositivos médicos que monitoram sinais vitais, sensores que controlam as condições do solo na agricultura e inúmeras ferramentas que compõem a infraestrutura urbana. Diante da sua integração na vida cotidiana, a IoT enseja a troca constante de dados pessoais que, muitas vezes, ultrapassam as fronteiras.

As tecnologias analisadas permitem notar que a conectividade da Internet serve como motor para que possam operar. Embora faça parte das TIC, a análise da Internet merece atenção especial e será, por consequência, conduzida de forma separada na Seção seguinte.

---

38 MILLARD, Christopher J. **Cloud computing law**. Oxford: Oxford University Press, 2021.

39 MILLARD, 2021. p. 7.

40 TREACY, Bridget; BAPAT, Anita. The Internet of Things – already in a home near you? **Privacy and Data Protection,** v. 14, n. 2, 2013. pp. 11-13. Disponível em: https://www.hunton.com/images/content/3/4/v2/3421/The_Internet_of_Things_already_in_a_home_near_you.pdf. Acesso em: 2 nov. 2023.

1.1.3. Internet

À medida que os dados pessoais estão cada vez mais disponíveis, a Internet é a principal rede que viabiliza a sua transposição por sobre as fronteiras. Não sem razão, o Fórum Econômico Mundial destacou que o mundo virtual está inundado de dados pessoais.[41] A evolução da Internet moderna, tal como a conhecemos hoje, resultou de um processo de desenvolvimento contínuo e progressivo ao longo do tempo. A década de 1990 marcou o início de uma fase de expansão, permitindo o uso da Internet por um público mais amplo à medida que ferramentas básicas e computadores pessoais passaram a se tornar acessíveis para que qualquer pessoa pudesse se conectar à rede. Segundo Manuel Castells, a Internet é um símbolo da sociedade moderna e, atualmente, as principais atividades econômicas, sociais, políticas e culturais estão estruturadas na rede.[42]

Jürgen Feick e Raymund Werle argumentam que o crescimento da Internet para uma rede global só foi possível devido ao atendimento de requisitos operacionais essenciais para que esse sistema descentralizado funcionasse de forma coesa, os quais incluem compatibilidade, identificação e interconectividade. A compatibilidade facilita a integração das redes e é alcançada por meio de padrões técnicos. A identificação é garantida pela atribuição de endereços únicos a usuários ou objetos nas redes. A interconectividade implica o compromisso ou a obrigação dos provedores ou operadores em conectar suas redes, conforme os requisitos de compatibilidade e identificação.[43]

Embora a definição da Internet seja predominantemente técnica, é importante destacar alguns aspectos. Em 1995, o Conselho Federal de Redes dos Estados Unidos (*Federal Networking Council*, FNC) descreveu a Internet como um sistema global de informação que está logicamente interligado por um espaço de endereçamento único global baseado no Protocolo de Internet (IP), que é capaz de suportar comunicações usando o conjunto de Protocolo de Controle de Transmissão/Protocolo de Internet (TCP/IP) e que fornece, utiliza ou torna acessível, de forma pública ou privada, serviços

---

41 WORLD ECONOMIC FORUM. **Personal Data: The Emergence of a New Asset Class**. 2011. Disponível em: https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf. Acesso em: 2 nov. 2023.

42 CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 2005.

43 FEICK, Jürgen; WERLE, Raymund. Regulation of cyberspace. In: BALDWIN, Robert; CAVE, Martin; LODGE, Martin (Ed.). **The Oxford handbook of regulation**. Oxford Handbooks, 2010.

com base nessa infraestrutura de comunicação.[44] Segundo Christopher Kuner, a referida definição tem como foco o uso de TCP/IP para distinguir a Internet de outras redes.[45] No entanto, a Internet vai além de um único protocolo técnico e envolve a interconexão das redes de comunicações e informações eletrônicas ao redor do mundo. Para o autor, uma definição mais ampla que englobe tais redes, não limitadas ao TCP/IP, é mais apropriada.

Sob essa perspectiva, a Internet pode ser considerada a "rede das redes", abrangendo as redes de comunicação e informação globais, sua infraestrutura e conteúdos interconectados e transmitidos por ela.[46] Para ilustrar esse ambiente, a literatura jurídica assinala que a estrutura da Internet funciona com base em camadas.[47-48-49] A camada de infraestrutura representa os meios para se conectar e acessar à Internet. Por seu turno, a camada lógica contém os protocolos e mecanismos por meio dos quais a Internet opera. Paralelamente, a camada de conteúdo abrange os dados e as informações que são transmitidas pela Internet e as normas jurídicas que estabelecem como eles podem ser usados, incluindo temas importantes, como a pornografia infantil, discurso de ódio e discriminação contra minorias e, de forma geral, permissões ou restrições ao fluxo de dados e de informações. A camada social, por fim, compreende as práticas que definem as condutas sociais na Internet. [50] Enquanto as primeiras camadas têm um caráter técnico, as últimas possuem um caráter jurídico-social.[51]

1.1.4. Contribuições das teorias de regulação da Internet para o debate sobre transferências internacionais de dados pessoais

As discussões sobre a regulação da Internet têm acompanhado o seu contínuo processo de transformação e perpassam por questionamentos sobre se a regulação jurídica estatal seria suficiente, adequada e eficaz para controlar o comportamento em um ambiente frequentemente denominado pela literatura jurídica como "ciberespaço".[52] A

---

44 FEDERAL NETWORKING COUNCIL. Definition of "Internet". **Resolution of 24 October 1995**. Disponível em: https://www.nitrd.gov/historical/fnc/internet_res.pdf. Acesso em: 2 nov. 2023.

45 KUNER, Christopher. The Internet and the global reach of EU law. In: CREMONA, Marise and SCOTT, Joanne (Eds.), **EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law**, 2017. pp. 112-145.

46 KUNER, 2017. p. 118.

47 KUNER, 2017. p. 119.

48 BENKLER, Yochai. **The wealth of networks: How social production transforms markets and freedom**, New Haven and London: Yale University Press, 2006. p. 515.

49 ZITTRAIN, Jonathan. **The future of the internet and how to stop it**. Yale University Press, 2008.

50 KUNER, 2017. p. 119.

51 FEICK; WERLE, 2010. p. 365.

52 GELLMAN, Robert. Can privacy be regulated effectively on a national level? Thoughts on the possible need for international privacy rules. **Villanova Law Review**, v. 41, 1996, pp. 129-172. Disponível em: https://digitalcommons.law.villanova.edu/vlr/vol41/iss1/2/. Acesso em: 2 nov. 2023.

regulação pela atividade normativa estatal lida com um mundo demarcado por fronteiras físicas em que os indivíduos vivem sob a jurisdição de normas locais e de suas autoridades correspondentes. Essas normas e autoridades constituem os sistemas jurídicos nacionais, que criam obrigações dentro de uma área específica.[53] No entanto, o ciberespaço é descrito como um ambiente global caracterizado pela ausência de limitações geográficas, no qual as atividades são conduzidas por meio da infraestrutura tecnológica da Internet. Nesse cenário, não há espaço físico definido, mas um ambiente virtual que possibilita uma variedade de interações.[54] Assim, diante do seu caráter transnacional, as atividades no ciberespaço podem envolver indivíduos que estão sujeitos a sistemas jurídicos em diferentes regiões ao redor do mundo, além da sobreposição de leis nacionais.

A compreensão do ciberespaço desafia paradigmas tradicionais, como jurisdição, territorialidade e soberania. Na fase inicial do debate sobre regulação do ciberespaço, Jonh Perry Barlow, responsável pela emblemática Declaração de Independência do Ciberespaço, em 1996, defendeu que o ciberespaço deveria permanecer livre da influência estatal.[55] Ele e outros defensores do ciberlibertarianismo,[56] como David R. Johnson e David Post, argumentaram que a inexistência de fronteiras geográficas impossibilitava a atividade normativa estatal.[57] A conclusão era de que o ciberespaço seria um ambiente insuscetível de regulação. Como contraponto a esse movimento, não demorou muito para que outros autores passassem a avaliar possíveis soluções para a regulação do comportamento no ciberespaço. Embora o ciberespaço seja um ambiente virtual, seus protocolos e demais camadas são operados por seres humanos, que são influenciados por estratégias de coerção e poder.[58] Como aponta Tim Wu, o ciberespaço também pode estar sujeito às forças regulatórias que moldam a história humana, não estando isolado ou imune a essas influências.[59]

---

53 REMOLINA, Nelson. **Recolección internacional de datos personales: un reto del mundo post-internet**. XVIII Edición del Premio Protección de Datos Personales de Investigación. Madrid: Agencia Española de Protección de Datos, 2015. pp. 294-295.

54 LESSIG, Lawrence. **Code: version 2.0**. Nova Iorque: Basic Books, 2006.

55 BARLOW, John Perry. **Declaration of independence for cyberspace**. 8 fev.1996. Disponível: https://www.eff.org/cyberspace-independence. Acesso em: 2 nov. 2023.

56 MURRAY, Andrew. **The regulation of cyberspace: control in the online environment**. Routledge, 2007.

57 JOHNSON, David R.; POST, David. Law and borders: The rise of law in cyberspace. **Stanford law review**, 1996. pp. 1367-1402.

58 KELLER, Clara Iglesias. Entre exceção e harmonização: o debate teórico sobre a regulação da Internet| Between exception and harmonization: the theoretical debate on Internet regulation. **Revista Publicum**, v. 5, n. 1, 5 nov. 2019. pp. 137-166.

59 WU, Tim. Is Internet Exceptionalism Dead? In: SZOKA, Berim e MARCUS, Adam (Eds.) **The Next Digital Decade: Essays on The Future of Internet**. Washington DC: TechFreedom, pp. 179-188. 2010. p. 180

Em 1998, Joel R. Reidenberg propôs uma conexão da teoria jurídica do ciberespaço à *Lex Mercatoria,* processo que ele denominou de *Lex Informatica.*[60] Segundo o autor, a intervenção estatal não seria a única fonte para a atividade regulatória, que também envolveria o setor privado, com os desenvolvedores técnicos e os usuários.[61] Reidenberg reconheceu que a existência de diferentes leis nacionais de países poderia trazer obstáculos para os fluxos transfronteiriços de dados no ciberespaço.[62] Nesse sentido, a proposta da *Lex Informatica* busca complementar a regulação estatal, incluindo padrões técnico-jurídicos e destacando a arquitetura da rede como mecanismo regulatório capaz de intervir nos fluxos de informações, independentemente de delimitações geográficas. Isso resolveria a aparente incompatibilidade da regulação do ciberespaço devido à sobreposição de diferentes leis nacionais.[63]

Mais tarde, o conceito da *Lex Informatica* foi utilizado por Lawrence Lessig para construção do seu conceito de *Code* como força regulatória no ciberespaço.[64] No seu trabalho, Lessig argumenta que a atividade normativa jurídica realizada pelos Estados não é suficiente no ciberespaço. Ele defende que as constrições sociais, o mercado e a arquitetura são igualmente importantes para intervir nesse ambiente. A sua proposta é que a regulação envolve uma combinação desses fatores, não apenas a lei.[65] As constrições sociais podem moldar o comportamento por meio de práticas e da confiança. O mercado pode impor restrições segundo a lógica da oferta e da demanda. A arquitetura, por sua vez, constitui a própria base para a construção do ciberespaço na forma de códigos. Diferentes atores, incluindo desenvolvedores técnicos e usuários, podem reconfigurar o código para reproduzir elementos do mundo físico, tais como barreiras e limites. O código, portanto, seria a forma mais eficaz de estimular ou restringir comportamentos no ciberespaço, pelo fato de poder defini-los antes mesmo de ocorrerem. É por essa razão que Lessig afirma que o código desempenha o papel de lei no ciberespaço.[66]

---

60 REIDENBERG, Joel R. Lex informatica: The formulation of information policy rules through technology. **Texas Law Review**, v. 76, n. 3, 1998. pp. 553-593.Disponível em: https://core.ac.uk/download/pdf/144222024.pdf. Acesso em: 2 nov. 2023.

61 REIDENBERG, 1998. pp. 568-569.

62 REIDENBERG, Joel R. Governing networks and rulemaking in Cyberspace. **Emory Law Journal**, v. 45, 1996. pp. 911-930. Disponível em: https://ir.lawnet.fordham.edu/faculty_scholarship/29. Acesso em: 2 nov. 2023.

63 REIDENBERG, 1998. pp. 570-572.

64 LESSIG, 2006. p. 5.

65 LESSIG, 2006. pp.123-125.

66 LESSIG, 2006. p. 223.

Andrew Murray leva a proposta de Lessig um passo adiante, focando no fluxo dinâmico e interativo da informação no ciberespaço.[67] Assim como Lessig, ele sugere quatro fatores que influenciam a regulação, sendo eles: o controle hierárquico, competitivo, comunitário e por arquitetura. No entanto, Murray assinala que a regulação é policêntrica. Isso significa que o destinatário da regulação não é meramente passivo às forças regulatórias, mas também é um ator que participa ativamente nesse ambiente complexo. A distinção entre reguladores e regulados torna-se menos evidente, uma vez que ambos desempenham essas funções simultaneamente.

Esse fenômeno acontece pois os atores reguladores são parte de comunidades no ciberespaço e delas obtém sua legitimidade.[68] Ainda, Murray destaca que as comunidades no ciberespaço possuem *gatekeepers* que surgem de pontos críticos no fluxo de informação e têm o poder de exercer influência no ambiente regulatório.[69] Nesse sentido, a regulação se desenvolve de forma orgânica e simbiótica. Os controles hierárquico, competitivo e comunitário são considerados de primeira ordem na regulação. Embora o controle por arquitetura seja poderoso, é considerado de segunda ordem, tendo em vista que a sua eficácia depende do reconhecimento e aceitação com base nos controles de primeira ordem. A partir dessa reflexão, a principal consequência extraída é a relevância de estratégias híbridas de regulação.[70]

As comunidades no ciberespaço também foram objeto de estudo por Paul S. Berman ao avaliar a globalização e o pluralismo.[71] Berman argumenta que as comunidades se originam a partir de uma identificação simbólica e de psicologia social, não sendo definidas por demarcações territoriais. Essa compreensão dinâmica da relação entre as comunidades nacionais e outras formas de afiliação transnacionais e internacionais permite conceituar jurisdição como processos fluidos de interações sociais, que não se limita às fronteiras territoriais rígidas. A concepção em questão de jurisdição está situada entre o territorialismo e o universalismo. Mesmo que este último possa parecer uma opção válida à primeira vista, Berman pondera a sua inadequação para o

---

67 MURRAY, 2007. pp. 34-35.
68 MURRAY, 2007. pp. 47-51.
69 MURRAY, Andrew. Nodes and gravity in virtual space. **Legisprudence: International Journal for the Study of Legislation, Hart Pub**, v. 5, n. 2, out. 2001, pp.195-221.
70 MURRAY, Andrew. Conceptualising the Post-Regulatory (Cyber)state. In: BROWNSWORD, Roger, YEUNG, Karen (org). Regulating technologies: **legal futures, regulatory frames and technological fixes**. Oxford, Hart, 2008. pp. 287-316.
71 BERMAN, Paul Schiff. The globalization of jurisdiction. **University of Pennsylvania Law Review**, v. 151, n. 2, dez. 2002, pp. 311-545. Disponível em: https://core.ac.uk/download/pdf/192849822.pdf. Acesso em: 2 nov. 2023.

ciberespaço, considerando que o universalismo pressupõe um ponto de identificação à parte do contexto social e cultural. Além disso, com base na concepção de jurisdição proposta, reconhece-se que as normas jurídicas não derivam exclusivamente dos comandos coercitivos de um poder soberano, sendo construídas a partir da concorrência de comunidades mediante processos transnacionais. Assim, as comunidades desempenham um papel fundamental na criação do Direito.[72]

As teorias de regulação do ciberespaço abordadas trazem três elementos importantes para os desafios transnacionais no ambiente virtual. O primeiro leva à constatação das diferentes forças regulatórias do ciberespaço e da possibilidade de a arquitetura, por si só, atuar como uma dessas forças. Nesse sentido, a forma como o ciberespaço é projetado pode estabelecer regras de comportamento para os usuários para alcançar os objetivos almejados. O segundo consiste em reconhecer a diversidade de agentes envolvidos na regulação do ciberespaço, abrangendo múltiplos atores e comunidades que influenciam o fluxo de informações, tais como Estados, setor privado, sociedade civil, organizações intergovernamentais, comunidade acadêmica e técnica.[73] O terceiro diz respeito a estratégias regulatórias híbridas que podem ser oferecidas pela articulação desses múltiplos atores, seja como reguladores, seja como regulados. Como resultado, o ciberespaço apresenta novos instrumentos e estratégias para a regulação e atribui poder regulatório a entidades e organizações que tradicionalmente têm sido os alvos da regulação.

De forma ampla, tornou-se evidente que a regulação tem mpacto nas tecnologias, mas também é afetada por elas. As soluções tecnológicas alteram não apenas as questões, o objeto e as circunstâncias da regulação, mas também seus instrumentos e estratégias, incluindo os aspectos sobre quem tem capacidade e legitimidade para regular.[74] Enquanto há debates que defendem que as tecnologias são neutras ou puramente técnicas, outros contrapõem afirmando que essas soluções incorporam interesses

---

[72] JOERGES, Christian; SAND, Inger-Johanne; TEUBNER, Gunther (Ed.). **Transnational governance and constitutionalism**. Hart Publishing, 2004.

[73] BLACK, Julia. Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. Current Legal Problems, v. 54, n. 1, **Oxford University Press (OUP)**. fev. 2001, pp. 103-146. Disponível em: https://academic.oup. com/clp/article-abstract/54/1/103/400274?redirectedFrom=fulltext. Acesso em: 2 nov. 2023.

[74] FEICK; WERLE. 2010. p. 364.

comerciais, inclinações políticas e avaliações morais.[75-76] Neste último caso, Julie Cohen assinala que as tecnologias são moldadas pelos valores e prioridades de seus desenvolvedores e detentores. [77] Ela adverte que a concepção da tecnologia, como um instrumento neutro, pode ameaçar a sua sujeição a controles democráticos, sendo necessário preservar espaços regulatórios tanto jurídicos quanto técnicos.[78]

Como analisado nas Seções acima, os desenvolvimentos das TIC, aliados à Internet, motivou discussões sobre a regulação jurídica dos dados pessoais. As prescrições jurídicas, no entanto, podem variar consideravelmente de um país para outro em razão das suas diferentes tradições jurídicas, históricas e culturais, além de se sobreporem no espaço virtual, o que impõe desafios às transferências internacionais de dados pessoais.[79-80] Para alcançar uma solução comum em termos de regulação jurídica, o Direito Internacional e a celebração de tratados internacionais são tradicionalmente buscados. A despeito de um movimento internacional e regional para a promoção de padrões de conformidade comuns, que será examinado na Seção 1.2, não se constata a existência de um tratado adotado globalmente sobre a proteção dos dados pessoais. Pelo contrário, conforme será analisado na Seção 1.2, as diferenças entre os modelos regulatórios da UE e dos EUA, têm provocado fortes tensões para a transferência transatlântica de dados pessoais.

Devido a isso, é notório o valor das contribuições das teorias de regulação da Internet para enfrentar questões transnacionais. Sob essa perspectiva, regimes jurídicos interoperáveis para a tutela das transferências internacionais de dados pessoais[81] tendem a ser melhor efetivados a partir de um modelo regulatório híbrido, em que a responsabilidade é distribuída entre os diversos atores envolvidos na regulação para a

---

75 HOOD, Christopher. The tools of government in the information age. In: MORAN, Michael; REIN, Martin; GOODIN, Robert E. (Ed.). **The Oxford handbook of public policy**. Oxford University Press, 2008. pp.469–481.

76 FRAZÃO, Ana. **Premissas para a reflexão sobre a regulação da tecnologia**. JOTA, 16 nov. 2017. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/premissas-para-a-reflexao-sobre-a-regulacao-da-tecnologia-16112017. Acesso em: 2 nov. 2023.

77 COHEN, Julie E. What privacy is for. **Harvard Law Review**., v. 126, 2013. pp. 1904-1933.

78 COHEN, 2013. p.1929.

79 BERMAN, Paul Schiff. Global legal pluralism. **Southern California Law Review**, v. 80, n.6, 2007, pp. 1155-1238.

80 BERMAN, Paul Schiff. Global legal pluralism as a normative project. **UC Irvine La Review**, v. 8 mar. 2018, pp. 149-181.

81 WEBER, Rolf H. 2014, p. 20.

criação e aderência às normas.[82] A corregulação pode ser alcançada com a elaboração de normas e diretrizes gerais pela atividade estatal que permitem que agentes privados tenham espaço de atuação e complementação.[83-84] Da mesma forma, a corregulação compreende o incentivo de regras e práticas elaboradas por entes privados que estão sujeitos à aprovação e/ou supervisão de autoridades estatais, como as APD.[85] A relevância de um modelo de corregulação com capacidade de aplicar penalidades para a tutela efetiva da proteção de dados também é digna de nota, dada a insuficiência da autorregulação isolada. Na direção de um modelo regulatório híbrido, destacam-se instrumentos e estratégias que contemplam a arquitetura, a responsabilidade e prestação de contas dos agentes envolvidos (em inglês, *accountability*) e o dimensionamento de riscos associados às transferências internacionais de dados pessoais.[86]

Com relação à regulação pela arquitetura, a delimitação de padrões técnicos para a proteção dos dados pessoais, inclusive como mecanismos para viabilizar as transferências internacionais de dados pessoais, tem sido objeto de trabalho de organizações de padronização como *International Standards Organization* (ISO), *European Committee for Standardization* (CEN), *European Telecommunications Standards Institute* (ETSI).[87] A série ISO/IEC 27000,[88] que inclui a ISO/IEC 27018 sobre proteção de dados em serviços de nuvem, pode ser considerada um exemplo dessas iniciativas. O *Electrical and Electronics Engineers Standards Association* (IEEE-SA), por sua vez, está à frente de diversos processos para estabelecer padrões técnicos em áreas como tecnologia da informação, robótica, entre outros. No entanto, conforme elucidam Colin Bennett e Charles Raab, o reconhecimento efetivo de padrões técnicos como

---

82 MENDES, Laura Schertel; DA FONSECA, Gabriel C. Soares. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **REI-Revista Estudos Institucionais**, v. 6, n. 2, mai/ago. 2020. pp. 507-533.

83 SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 21 ago. 2019. p. 240.

84 MARSDEN, Christopher T. Internet Co-regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace**.** Cambridge: **Cambridge University Press**, 18 ago. 2011.

85 ARANHA, Marcio Iorio; LOPES, Othon. **Estudo sobre Teorias Jurídicas da Regulação apoiadas em incentivos**. Pesquisa e Inovação Acadêmica sobre Regulação apoiada em Incentivos na Fiscalização Regulatória de Telecomunicações, ANATEL/UnB, 2019.

86 SOMBRA, 2019. p. 240.

87 BENNETT, Colin; RAAB, Charles D. **Revisiting "The Governance of Privacy":** Contemporary Policy Instruments in Global Perspective. 17 ago. 2018. pp. 9-10. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972086. Acesso em: 2 nov. 2023.

88 IT GOVERNANCE. **ISO 27700 Privacy Information management system**. Green paper. 2023. Disponível em: https://www.itgovernance.co.uk/iso-27701. Acesso em: 2 nov. 2023.

instrumentos para a conformidade regulatória tem sido relativamente lenta e ponderada.[89] Dessa forma, o exame de tais padrões técnicos não será aprofundado nesta pesquisa.

A despeito disso, cabe pontuar as Tecnologias de Aprimoramento da Privacidade (em inglês, *Privacy Enhancing Technologies* ou PETs), que são desenhadas para fortalecer a proteção e a segurança dos dados pessoais, como é o caso da criptografia, que permite que apenas os interlocutores da comunicação possam acessar as informações. Além dessas tecnologias, Ann Cavoukian explora o conceito de privacidade pelo design (em inglês, *privacy by design*).[90] Cavoukian argumenta que a proteção da privacidade e dos dados pessoais deve ser uma prática inerente à operação das organizações. Inicialmente, a noção de privacidade pelo design focava em integrar a privacidade desde o início do desenvolvimento de soluções tecnológicas. Com o tempo, essa abordagem evoluiu para um modelo holístico que visa a criar programas de proteção da privacidade e dos dados pessoais abrangentes.[91]

A abordagem ampliada pode ser aplicada não apenas em sistemas de tecnologia da informação para garantir que sejam projetados para proteger a privacidade desde a sua concepção, mas também nas práticas de negócios e operações, nos *designs* físicos e de infraestrutura. Outro parâmetro que ganhou destaque é a privacidade por padrão (em inglês, *privacy by default)*, que trata da predefinição de configurações de privacidade e proteção de dados mais rígidas. Como sustenta Paul M. Schwartz, o objetivo é garantir que a opção com maior grau de proteção seja oferecida por padrão, por exemplo, com a coleta de dados pessoais limitados à quantidade mínima necessária, mesmo que em alguns casos os indivíduos tenham espaço para exercer as suas preferências por opções menos rigorosas.[92]

Além da arquitetura, a responsabilidade e prestação de contas também pode ser introduzida como instrumentos capazes de regular a proteção de dados e as transferências internacionais de dados pessoais.[93] A definição de responsabilidade e

---

89 BENNETT; RAAB, 2018. p. 10.

90 CAVOUKIAN, Ann. **Privacy by design: take the challenge**. Toronto: Information and privacy commissioner of Ontario (Canada), 1 jan. 2009.

91 CAVOUKIAN, Ann; TAYLOR, Scott; ABRAMS, Martin E. Privacy by design: essential for organizational accountability and strong business practices. **Identity in the Information Society**, v. 3, n. 2, 4 ago. 2010. pp.405-413. Disponível em: https://core.ac.uk/download/pdf/81526429.pdf. Acesso em: 2 nov. 2023.

92 SCHWARTZ, Paul M. Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices. **Wisconsin Law Review**, 2000. pp. 743-788.

93 CENTRE FOR INFORMATION POLICY LEADERSHIP. **What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework**. Report of the CIPL Accountability Mapping Project, mai. 2020. Disponível em:

prestação de contas é fundamentada em dois aspectos principais. O primeiro refere-se à obrigação de uma entidade de explicar (prestar contas) como cumpriu certas responsabilidades ou as razões por ter agido de determinada maneira. O segundo sugere a existência de uma relação na qual uma entidade é responsável perante outra.[94] Esses aspectos encontraram expressão na proteção de dados por meio da implementação e fiscalização de salvaguardas concretas pelos diferentes atores envolvidos nas atividades de tratamento, o que contribui para a transição da proteção "da teoria para a prática". As salvaguardas incorporam não apenas uma postura reativa, em que os agentes são instados após o surgimento de reclamações, mas também proativa, permitindo que sejam solicitados a evidenciar a conformidade antes de qualquer alegação de inadequação.[95]

Outro ponto a destacar é a adoção de avaliações para o dimensionamento de riscos e de danos associados ao tratamento de dados pessoais e, mais especificamente às transferências internacionais de dados pessoais, como instrumentos de regulação. A literatura jurídica tem definido diferentes categorias e subcategorias sob as lentes de potenciais riscos e danos que podem ser causados aos titulares, incluindo a perda de controle sobre os dados pessoais, o roubo de identidade, a assimetria informacional,[96] o tratamento discriminatório com base em dados pessoais, entre outros.[97] Essas categorias servem para que os diferentes atores envolvidos no tratamento possam avaliar o grau de probabilidade de ocorrência de eventos que ameaçam ou impactam a proteção dos dados dos titulares. Isso permite desenvolver estratégias não apenas para mitigar os efeitos, mas para antecipá-los e preveni-los. Além disso, as avaliações de riscos e danos podem ser moldadas pelas características e pelo contexto das atividades, permitindo a adoção de medidas adaptáveis e compatíveis ao grau do risco.[98]

Como será analisado na Seção seguinte, os instrumentos e estratégias regulatórias discutidos acima foram abordados ao longo de iniciativas lideradas por organizações internacionais e regionais, e blocos econômicos para a construção de padrões comuns de conformidade jurídica de proteção de dados, que foram

---

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_mapping_long_infographic.pdf. Acesso em: 2 nov. 2023.

94 ALHADEFF, Joseph; VAN ALSENOY, Brendan; DUMORTIER, Jos. The accountability principle in data protection regulation: origin, development and future directions. In: **Managing privacy through accountability**. London: Palgrave Macmillan UK, 2012. pp. 49-82.

95 ALHADEFF; VAN ALSENOY; DUMORTIER, 2012. p. 76.

96 PASQUALE, Frank. The black box society. The secret algorithms that control money and information. Cambridge: **Harvard University Press**. 2015.

97 BENNETT; RAAB, 2018. pp 31-33.

98 NISSENBAUM, Helen. Privacy in context: Technology, policy, and the integrity of social life. **Stanford University Press**, 2020.

impulsionadas, sobretudo, para garantir que as transferências internacionais de dados pessoais não fossem impossibilitadas.

1.2. O panorama sobre as transferências internacionais de dados pessoais em instrumentos internacionais e regionais

As transferências internacionais de dados pessoais representam um dos fatores preponderantes para os esforços voltados para a interoperabilidade jurídica da regulação da proteção de dados ao redor do mundo. Ainda que as preocupações entre os diferentes países apresentem nuances próprias, desde os anos 1970, tem-se desenvolvido uma agenda em torno da construção de padrões comuns de conformidade para, de um lado, garantir a proteção global dos dados pessoais e, de outro, eliminar barreiras injustificadas para a sua circulação. O intuito é evitar que as distintas respostas normativas à proteção de dados se convertam em obstáculos para os fluxos de dados pessoais ou reduzam os seus padrões de proteção.[99]

Ao longo desse movimento, vêm sendo produzidos instrumentos internacionais e regionais caracterizados por diferentes naturezas e efeitos jurídicos. Como delineado nos trabalhos de Colin Bennett e Charles Raab, tais instrumentos ensejaram uma convergência regulatória para solucionar problemas comuns envolvendo o tratamento e a transferência internacional de dados pessoais, que tende a se refletir nas leis nacionais sobre o tema.[100] Esta Seção oferece um panorama desse processo, abordando historicamente os documentos jurídicos pertinentes para esta pesquisa.

1.2.1. O núcleo comum de princípios de proteção de dados

No decorrer das discussões relativas à proteção de dados, consolidou-se um conjunto de princípios para orientar as atividades de tratamento, denominados de *Fair Information Principles*.[101] A origem de tal núcleo principiológico remete ao relatório produzido pelo governo federal dos EUA em 1973, no âmbito do Departamento de Saúde, Educação e Bem-Estar (em inglês, *Department of Health, Education, and Welfare*), que

[99] REMOLINA, 2015. pp. 152-153.

[100] BENNETT, Colin; RAAB, Charles D. **The governance of privacy: Policy instruments in global perspective**. First published 2003, Routledge Revivals, 2018(b).

[101] GELLMAN, Robert. **Fair Information Practices: a basic History**, 2022. p. 59. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020. Acesso em: 2 nov. 2023.

concluiu pela necessidade de estabelecer as seguintes regras de controle sobre os dados pessoais:[102]

> - Não deve existir nenhum sistema de manutenção de registros de dados pessoais cujo existência seja secreta.
> - Deve existir um meio para que um indivíduo descubra qual informação sobre si está registrada e como ela é usada.
> - Deve existir um meio para que um indivíduo possa prevenir que informação sobre si, obtida para um determinado propósito, seja usada ou disponibilizada para outros propósitos sem o seu consentimento.
> - Deve existir um meio para que um indivíduo possa corrigir ou emendar um registro de informação identificável sobre si.
> - Qualquer organização que cria, mantém, usa ou dissemina registros de dados pessoais identificáveis deve garantir a confiabilidade desses dados para o uso definido e deve tomar precauções para prevenir o uso indevido deles (tradução livre).

Além disso, o Apêndice B desse documento apresentava um quadro dos debates sobre a proteção de dados que vinham sendo desenvolvidos em outros países, destacando preocupações comuns relacionadas ao uso de sistemas computacionais de dados pessoais e os seus efeitos para além das fronteiras nacionais.[103] Conforme assinalado no relatório em questão, o Comitê de Privacidade do Reino Unido havia conduzido na mesma época um estudo detalhado que resultou na sugestão de medidas para tratar potenciais riscos associados a sistemas computacionais de dados pessoais geridos por entidades privadas, quais sejam:[104]

> - As informações devem ser armazenadas para uma finalidade específica e não devem ser utilizadas para outras finalidades, sem a devida autorização;
> - O acesso às informações deve ser conferido àqueles que têm a autorização de mantê-lá com os fins pelos quais elas foram coletadas;
> - A quantidade de informações coletadas e armazenadas deve ser o mínimo necessário para se alcançar um objetivo específico;
> - Em sistemas computadorizados que processam informações com fins estatísticos, devem ser tomadas medidas adequadas em seu *design* e programas para separar a identidade do restante dos dados;
> - Deve haver mecanismos pelos quais o sujeito possa ser comunicado sobre a informação armazenada a seu respeito;
> - O nível de segurança que um sistema deve alcançar deve ser especificado previamente pelo usuário e deve incluir precauções contra abusos deliberados ou mau uso da informação;
> - Um sistema de monitoramento deve ser provido para facilitar a detecção de qualquer violação da segurança do sistema;
> - No *design* de sistemas de informação, devem ser especificados períodos para além dos quais a informação não pode mais ser retida;
> - Os dados armazenados devem ser precisos. Deve haver instrumentos para a retificação de imprecisões e para a atualização da informação;

---

[102] ESTADOS UNIDOS. **Records, computers, and the rights of citizens**. Washington, DC: Department of Health, Education & Welfare, 1973. pp. XX-XXI. Disponível em: https://www.justice.gov/opcl/docs/rec-com-rights.pdf. Acesso em: 2 nov. 2023.

[103] ESTADOS UNIDOS, 1973. p. 167.

[104] GREAT BRITAIN, Home Office, **Report of the Committee on Privacy**. Rt. Hon. Kenneth Younger, Chairman (London: H. M. Stationery Office), 1972.

- Deve ser tomado cuidado na codificação de julgamentos de valor (tradução livre).

A partir de então, essas práticas passaram a encontrar expressão sob a forma de um quadro comum de princípios a serem aplicados na proteção de dados, previstos em instrumentos internacionais e regionais e em legislações nacionais subsequentes, como é o caso da Lei do Estado de Hesse de 1975, na Alemanha, conhecida como a primeira lei de proteção de dados do mundo. [105] Ainda que segmentados, condensados ou adaptados, os princípios constituem o alicerce da proteção de dados, delineando as questões centrais que devem ser enfrentadas para oferecer soluções para a temática.[106] É possível sintetizá-los nos seguintes termos:[107]

> Uma organização tanto pública quanto privada deve:
> - identificar as finalidades para as quais os dados são processados no momento da coleta ou antes dela;
> - coletar dados pessoais apenas com o conhecimento e consentimento do indivíduo, exceto sob circunstâncias especificadas;
> - limitar a coleta de dados pessoais àqueles que são necessários para alcançar os as finalidades identificadas;
> - reter os dados apenas pelo tempo necessário;
> - garantir que as informações pessoais sejam mantidas precisas, completas e atualizadas;
> - proteger as informações pessoais com salvaguardas de segurança apropriadas;
> - ser transparente sobre suas políticas e práticas e não manter nenhum sistema de informações secreto;
> - permitir que os titulares dos dados tenham acesso aos seus dados pessoais, com a capacidade de alterá-los se estiverem imprecisas, incompletas ou desatualizados;
> - ser responsável e prestar contas a respeito dos dados pessoais em sua posse.

A convergência internacional em torno desses princípios se torna evidente à medida que foram incorporados pelas mais variadas normativas em matéria de proteção de dados.[108] Assim, as Seções seguintes irão traçar os instrumentos internacionais e regionais que abordam os princípios.

1.2.2. Organização para a Cooperação e Desenvolvimento Econômico, OCDE

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) é uma organização internacional fundada em 1961 que proporciona aos seus Estados-membros um fórum para discutir, desenvolver e aperfeiçoar políticas econômicas e

---

[105] BIONI, Bruno; MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 2a ed. São Paulo: Thomson Reuters, 2020.

[106] DONEDA, 2011. pp. 99-101.

[107] BENNETT; RAAB, 2018(b). pp. 37-38.

[108] BIONI; MENDES; 2020. p. 161.

sociais.[109] Atualmente, a Colômbia integra os Estados-membros da OCDE e, em 2022, a organização abriu discussão para o processo de adesão da Argentina e do Brasil. [110-111]

Dentre os seus principais objetivos está a promoção de políticas para alcançar o mais alto crescimento econômico sustentável e emprego, e um aumento do padrão de vida nos Estados-membros, mantendo a estabilidade financeira e apoiando o desenvolvimento da economia mundial. Ainda, os objetivos incluem a contribuição para uma sólida expansão econômica tanto em Estados-membros quanto em não membros no processo de desenvolvimento econômico e para a expansão do comércio mundial de forma multilateral, não discriminatória e em conformidade com as obrigações internacionais.[112] Conforme será aprofundado a seguir, no decorrer do tempo, a OCDE desempenhou um papel fundamental na articulação de orientações relacionadas à proteção de dados e às transferências internacionais de dados pessoais.

1.2.2.1. Diretrizes de Privacidade da OCDE, de 1980

Em 1980, a OCDE emitiu o primeiro instrumento internacional sobre proteção de dados por meio das Diretrizes sobre a Proteção da Privacidade e o Fluxo Transfronteiriço de Dados Pessoais (Diretrizes de Privacidade). Essa iniciativa visava a contribuir com a harmonização das legislações nacionais sobre privacidade e proteção de dados e, ao mesmo tempo, fornecer um quadro para facilitar a livre circulação de dados pessoais. Apesar de abrangerem todos os meios de processamento, tanto no setor público quanto no privado, as Diretrizes de Privacidade da OCDE não têm caráter juridicamente vinculante.[113] Conforme descrito por Andrew Guzman e Timothy Meyer, as Diretrizes operam no âmbito de *soft law*, uma vez que, mesmo não sendo obrigatórias, buscam influenciar a formulação de políticas regulatórias.[114-115]

---

[109] BENNETT; RAAB, 2018(b). p. 111.

[110] OCDE. **Colombia's path towards OECD accession**. 15 jan. 2020. Disponível em: https://www.oecd.org/colombia/colombia-accession-to-the-oecd.htm. Acesso em: 2 nov. 2023.

[111] OCDE. **OECD takes first step in accession discussions with Argentina, Brazil, Bulgaria, Croatia, Peru and Romania**. 25 jan. 2022. Disponível em: https://www.oecd.org/newsroom/oecd-takes-first-step-in-accession-discussions-with-argentina-brazil-bulgaria-croatia-peru-and-romania.htm. Acesso em: 2 nov. 2023.

[112] OCDE. **Convention on the Organisation for Economic Cooperation and Development.** Paris, 14 dez. 1960. Disponível em: https://www.oecd.org/about/document/oecd-convention.htm. Acesso em: 2 nov. 2023.

[113] OCDE. **OECD Privacy Guidelines**. Paris, 23 set. 1980. Disponível em: https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en. Acesso em: 2 nov. 2023.

[114] GUZMAN, Andrew T.; MEYER, Timothy L. International soft law. **Journal of Legal Analysis**, v. 2, n. 1, 2010. pp. 171-225.

[115] CHANDER, Anupam; SCHWARTZ, Paul. Privacy and/or Trade. **U. Chi. L. Rev**., v. 90, 2023. p 49.

O preâmbulo expressa as principais preocupações que motivaram o estabelecimento das Diretrizes, reconhecendo que, embora as leis e políticas nacionais possam divergir, os Estados-membros têm um interesse comum em proteger a privacidade e as liberdades individuais e em conciliar valores fundamentais concorrentes como a privacidade e o livre fluxo de dados. Da mesma forma, sinaliza-se que o processamento automático e as transferências de dados criaram novas formas de relacionamento entre os países e passaram a requerer o desenvolvimento de regras e práticas compatíveis.[116]

A OCDE estabeleceu pela primeira vez um conjunto de princípios básicos para o tratamento de dados pessoais no âmbito de um instrumento internacional, os quais refletem um consenso de práticas que já vinham sendo reconhecidas para o tratamento adequado de dados, conforme analisado na Seção 1.2.1. Esses princípios incluem a limitação da coleta de dados, a necessidade de qualidade dos dados, a definição de finalidades para o uso dos dados, a segurança dos dados, a transparência sobre o tratamento dos dados, a existência de controles assegurados aos titulares dos dados, a responsabilização e prestação de contas por parte dos agentes que utilizam os dados.[117]

Com relação à circulação de dados, as Diretrizes de 1980 recomendam que os Estados-membros devem adotar todas as medidas razoáveis e apropriadas para garantir que as transferências internacionais de dados pessoais sejam ininterruptas e seguras. Nesse sentido, a recomendação é que os Estados-membro abstenham-se de restringir tais transferências de dados a outros Estados-membro, exceto quando o Estado-membro destinatário dos dados ainda não tenha observado substancialmente as Diretrizes ou a reexportação dos dados possa burlar a legislação local.[118]

Ainda, as Diretrizes de 1980 permitem que os Estados-membro imponham restrições às transferências em relação a certas categorias específicas de dados pessoais quando o Estado-membro destinatário não oferecer proteção equivalente. Não obstante, os Estados-membros devem evitar desenvolver leis, políticas e práticas que, visando a proteção da privacidade e das liberdades individuais, instituam barreiras às transferências internacionais de dados pessoais que excedem os requisitos necessários para tal proteção. Para a OCDE, a criação de barreiras injustificadas ou artificias do ponto de vista da

[116] OCDE, 1980. p. 11.
[117] OCDE, 1980. p. 14-16.
[118] OCDE, 1980. p. 16-17.

proteção da privacidade e dos dados poderiam ocasionar graves transtornos a setores da economia.[119]

À luz dessas recomendações, nota-se que, ao aderir às Diretrizes, o Estado destinatário dos dados passa a ter um status de proteção substancialmente similar ao do Estado de origem, indicando uma solução para a tutela das transferências internacionais de dados pessoais em um contexto intergrupo envolvendo os Estados-membros da OCDE.[120] Embora não estabeleça prescrições para as transferências realizadas a Estados não membros, o memorando explicativo das Diretrizes de 1980 reconhece que é desejável uma ampla aceitação das suas recomendações por Estados externos, considerando o crescimento das transferências de dados pessoais que transpõem as fronteiras nacionais e a necessidade de assegurar soluções coordenadas.[121]

Para implementar os princípios e recomendações em âmbito nacional, as Diretrizes de 1980 sugerem a criação de mecanismos legais e administrativos que garantam a proteção dos dados nas diferentes tradições jurídicas, incluindo a adoção de legislações adequadas, o incentivo e apoio à autorregulação, como códigos de conduta, o fornecimento de meios viáveis para os indivíduos defenderem seus direitos, e o estabelecimento de sanções e recursos, em caso de não conformidade. Além disso, as Diretrizes sublinham que os procedimentos para as transferências internacionais de dados pessoais e para a proteção da privacidade e dos dados sejam simples e compatíveis. Tais procedimentos devem facilitar a assistência mútua e a cooperação contínua entre autoridades e órgãos relevantes na temática.[122]

1.2.2.2. Diretrizes de Privacidade da OCDE, de 2013

As Diretrizes de Privacidade de 1980 foram revisadas no ano de 2013.[123] O início desse processo se deu entre 2010 e 2011, ocasião em que foram elaboradas análises sobre a necessidade de atualização do documento motivadas por mudanças em relação ao papel dos dados pessoais, bem como por novas abordagens para a proteção da privacidade que se desenvolveram com o passar dos anos.[124] Segundo o memorando explicativo da

[119] OCDE, 1980. p. 26.
[120] REMOLINA, 2015. p 179.
[121] OCDE, 1980. p. 33.
[122] OCDE, 1980. pp. 17-18.
[123] OCDE. **The OECD privacy framework**. Paris, 2013. p. 154. Disponível em: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso em: 2 nov. 2023.
[124] OCDE. **Thirty years after the OECD privacy guidelines**. Paris, 6 abr. 2011(a). p. 49. Disponível em: http://dx.doi.org/10.1787/5kgf09z90c31-en. Acesso em: 2 nov. 2023.

revisão feita em 2013, as Diretrizes de 1980 foram criadas em um contexto no qual as transferências de dados pessoais eram pontuais e discretas entre empresas e/ou Estados. No entanto, a situação evoluiu para um cenário no qual os dados podem ser tratados em múltiplos locais ao mesmo tempo, armazenados em diversos lugares ao redor do mundo e facilmente transportados por meio das fronteiras nacionais e em dispositivos móveis.[125]

O preâmbulo das Diretrizes de Privacidade da OCDE de 2013 renova a intenção de promover o livre fluxo de dados entre os Estados-membros e de evitar a criação de obstáculos injustificados para o desenvolvimento das relações econômicas e sociais entre eles. Para tanto, reconhece que os Estados-membros mantêm o interesse comum em promover e proteger os valores fundamentais de privacidade, liberdades individuais e do livre fluxo de dados. Além disso, adverte que a utilização extensiva e inovadora de dados pessoais pode trazer benefícios econômicos e sociais, mas também aumenta os riscos à privacidade. Nesse sentido, o texto ressalta que transferências contínuas de dados pessoais por meio de redes globais ampliam a necessidade de maior interoperabilidade entre os sistemas jurídicos, bem como de cooperação reforçada entre as APD. Por fim, evidencia a importância da avaliação de riscos no desenvolvimento de políticas e salvaguardas para proteger a privacidade e a existência de desafios para a segurança dos dados pessoais em um ambiente aberto e interconectado, no qual os dados pessoais são cada vez mais um ativo valioso.[126]

Embora os princípios básicos previstos no texto de 1980 tenham permanecido inalterados, as Diretrizes de 2013 trazem novos aspectos regulatórios.[127] Dentre eles, destaca-se a recomendação de estabelecer autoridades para a aplicação e fiscalização da proteção de dados com recursos e expertise técnica necessários para exercer seus poderes e tomar decisões de forma objetiva, imparcial e consistente.[128] Outro aspecto relevante refere-se à implementação de um enfoque baseado na responsabilidade dos agentes envolvidos no tratamento dos dados e na gestão de riscos, o que implica na criação e manutenção de programas bem estruturados com práticas de proteção dos dados.[129] Ainda, cabe ressaltar as recomendações destinadas a aprimorar a cooperação

---

OECD, Report on the Implementation of the OECD. **Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy**. Paris, 27 abr. 2011(b). p. 23. Disponível em: http://dx.doi.org/10.1787/5kgdpm9wg9xs-en. Acesso em: 2 nov. 2023.

[125] OCDE, 2013. p. 29.
[126] OCDE, 2013. pp. 11-12.
[127] OCDE, 2013. p. 4.
[128] OCDE, 2013. p. 28.
[129] OCDE, 2013. pp. 23-24.

internacional, o intercâmbio de informações entre APD e a interoperabilidade dos sistemas jurídicos.[130]

No que se refere à circulação de dados, as Diretrizes de 2013 estabelecem que o controlador permanece responsável pelos dados pessoais independentemente da localização de tais dados. Além disso, a redação prevista nas Diretrizes de 1980 é atualizada para estabelecer que qualquer restrição às transferências internacionais de dados pessoais imposta entre os Estados-membros deve ser proporcional aos riscos apresentados, considerando a sensibilidade dos dados, a finalidade e o contexto do tratamento.[131] As Diretrizes de 2013 ampliam também as soluções para a tutela das transferências internacionais de dados pessoais, especificando duas circunstâncias em que um Estado-membro deve se abster de impor restrições, quais sejam, quando o outro Estado-membro observar substancialmente as Diretrizes e quando existirem salvaguardas suficientes para assegurar um nível contínuo de proteção coerente com as Diretrizes.

Nesse último caso, o controlador poderá valer-se de estratégias combinadas, como salvaguardas de segurança técnica e organizacional, contratos e auditorias de conformidade de proteção de dados, entre outros. Ainda, deve-se implementar mecanismos caso essas estratégias se provem ineficazes, a exemplo de supervisão administrativa e judicial e de cooperação internacional entre as APD.[132] Com base na evolução de suas Diretrizes, portanto, a OCDE tem desempenhado um papel ativo nas discussões sobre transferências internacionais de dados pessoais e, até hoje, é um fórum influente no assunto.

1.2.3. Conselho da Europa

Com o término da Segunda Guerra Mundial, iniciou-se um período de construção de organismos internacionais focados em promover a paz e os direitos humanos, resultando na formação das Nações Unidas e, mais especificamente no contexto europeu, no Conselho da Europa.[133] Esse último foi fundado em 1949 por dez países europeus com a missão de fortalecer a democracia, os direitos humanos e o Estado de

[130] OCDE, 2013. pp. 33-34.
[131] OCDE, 2013. p. 30.
[132] OCDE, 2013. p. 29-31.
[133] VERONESE, Alexandre. Transferências internacionais de dados pessoais: o debate transatlântico norte e sua repercussão na América Latina e no Brasil. In: MENDES, Laura Schertel (coord.); DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); RODRIGUES JR., Otavio Luiza (coord.); BIONI, Bruno (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro Editora Forense, 2021. pp. 689-726.

Direito em todos os seus países membros.[134] Desde sua concepção, o Conselho da Europa reconhece que a defesa e a promoção de valores democráticos fundamentais transcendem as responsabilidades individuais dos governos, representando um compromisso coletivo e compartilhado entre todos os Estados-membros.[135]

O Conselho da Europa se destaca pela sua tradição na criação e implementação de instrumentos jurídicos internacionais que endereçam questões relacionadas ao desenvolvimento tecnológico. Na busca por reforçar suas ações, o Conselho da Europa estabeleceu parcerias com associações e empresas líderes no setor de tecnologia.[136] Outro ponto a frisar é que esses instrumentos do Conselho da Europa são tipicamente receptivos à participação de Estados não membros.[137]

A seguir, será apresentada uma visão geral das principais Convenções do Conselho da Europa que abordam a proteção de dados e as transferências internacionais de dados pessoais, e que representam compromissos multilaterais entre os seus signatários.

1.2.3.1. Convenção 108 do Conselho da Europa, de 1981

Logo após a promulgação das Diretrizes de Privacidade da OCDE, de 1980, o Conselho da Europa inaugurou o primeiro tratado internacional juridicamente vinculante no campo da proteção de dados pessoais, aplicável tanto ao setor público quanto ao privado, por meio da Convenção para a Proteção de Indivíduos em relação ao Tratamento Automatizado de Dados Pessoais, também conhecida como Convenção 108.[138] Esse tratado foi aberto à assinatura em 28 de janeiro de 1981, data em que se passou a celebrar o dia internacional da proteção de dados.

De forma progressiva, o documento foi sendo assinado e ratificado por Estados-membros e também por Estados externos, formando os Estados-partes, como é o caso da Argentina e do Uruguai. Atualmente, o Brasil constitui um observador do Comitê

---

134 BENNETT; RAAB, 2018, pp. 108-109.
135 BENNETT; RAAB, 2018, p. 109.
136 CONSELHO DA EUROPA. **Digital Partnerships**. 2023. Disponível em: https://rm.coe.int/leaflet-%20partnership-with-internet-companies-en/168079ced2%20. Acesso em: 2 nov. 2023.
137 GSTREIN, Oskar Josef. The Council of Europe as an Actor in the Digital Age: Past Achievements, Future Perspectives. **Festschrift der Mitarbeiter Innen und Doktorand Innen zum**, v. 60, 2019. pp. 75-90.
138 CONSELHO DA EUROPA. **Treaty 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. Estrasburgo, 28 jan. 1981. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108. Acesso em: 2 nov. 2023.

Internacional da Convenção. [139] O tratado não é autoexecutável, o que significa que os Estados-partes devem formular leis nacionais de proteção de dados para concretizar os seus fundamentos.[140] O seu preâmbulo não apenas reconhece a necessidade de conciliar a vida privada com a circulação de dados, mas também enfatiza a importância do respeito aos direitos humanos e às liberdades fundamentais. Sob essa perspectiva, a Convenção 108 possui três pilares, que incluem estabelecer princípios básicos para a proteção de dados, regular as transferências internacionais de dados pessoais e promover mecanismos de assistência mútua entre os Estados-partes.[141] O instrumento serve como base para os padrões europeus de proteção de dados, à luz dos direitos fundamentais.[142]

Nesse sentido, os Estados-partes devem adotar as medidas necessárias, em suas legislações internas, para implementar um conjunto de princípios básicos para o tratamento de dados pessoais, seguindo o consenso de práticas que vinham sendo reconhecidas no cenário internacional, conforme analisado nas Seções anteriores. Esses princípios referem-se, em particular, à coleta e ao processamento justo e lícito de dados; ao armazenamento de dados para finalidades legítimas e específicas e para a impossibilidade de uso incompatível com esses fins; à qualidade dos dados, os quais devem ser relevantes, proporcionais e precisos; e aos direitos de exercer o acesso, a retificação e a eliminação dos dados.[143]

O relatório explicativo da Convenção 108 reflete o receio de que os agentes busquem evitar controles de proteção de dados movendo suas operações, total ou parcialmente, para os denominados "paraísos de dados", isto é, países cujas leis de proteção de dados são menos rigorosas ou até mesmo inexistentes. Ao aderirem ao tratado, os Estados-partes poderiam resistir a uma tendência rumo a padrões de proteção inferiores.[144]

O artigo 12 da Convenção 108 estabelece prescrições para regular as transferências internacionais de dados pessoais e determina que um Estado-parte não deve proibir ou criar obstáculos para a transferência de dados pessoais a outro Estado-parte sustentando-se exclusivamente na necessidade de proteção dos mesmos. Nesse sentido, o

---

[139] CONSELHO DA EUROPA. Chart of signatures and ratifications of Treaty 108: **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.** 2023. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures. Acesso em: 2 nov. 2023.
[140] CHANDER; SCHWARTZ, 2023. p. 63.
[141] CONSELHO DA EUROPA, 1981 p. 1.
[142] GSTREIN, 2019. p. 83.
[143] CONSELHO DA EUROPA, 1981. pp. 2-4.
[144] CONSELHO DA EUROPA, 1981. p. 9.

dispositivo permite restrições à liberdade de transferência de dados pessoais em duas situações. Quando o Estado-parte originário tiver normas específicas de proteção para determinadas categorias de dados e o Estado-parte destinatário não oferecer padrão equivalente. E quando a transferência for para um Estado não signatário da Convenção, usando um intermediário que seja parte da Convenção. Essa última exceção tem como objetivo impedir manobras que busquem contornar as normas do Estado-parte mediante a utilização de intermediários.

Confira-se a redação do referido dispositivo:[145]

> Artigo 12. Fluxos de dados pessoais por sobre fronteiras e sistemas jurídicos nacionais.
> 1. As prescrições a seguir aplicar-se-ão às transferências de dados pessoais realizadas por qualquer meio – que estejam sendo tratados automaticamente ou que estejam sendo coletados com vistas a serem automaticamente tratados.
> 2. Um Estado-parte não poderá, com base somente na proteção à privacidade, proibir ou sujeitar a uma autorização especial os fluxos de dados pessoais remetidos ao território de outro Estado-parte.
> 3. No entanto, cada Estado-parte possui o direito de derrogar as prescrições do parágrafo (2), nos seguintes casos:
> a) na medida em que a sua legislação inclua prescrições regulatórias aplicáveis a categorias específicas de dados pessoais ou de arquivos de dados pessoais automatizados, em razão da natureza de tais dados ou arquivos, exceto quando as prescrições regulatórias do outro Estado-parte prover uma proteção equivalente;
> b) quando a transferência é realizada do seu território para o de outro Estado não partícipe da presente Convenção por meio da intermediação do território de outro Estado-parte, de modo a evitar que tais transferências resultem no contorno da legislação nacional do Estado-parte, referido no início do presente parágrafo (tradução livre).

Ao longo do anos, a Convenção 108 incorporou Protocolos Adicionais, que serão examinados na sequência.

1.2.3.2. Protocolo Adicional 181 do Conselho da Europa, de 2001

Com o aumento das transferências de dados pessoais por sobre as fronteiras, após duas décadas da sua emissão, a Convenção 108 foi complementada por meio do Protocolo Adicional 181 do Conselho da Europa, que foi aberto à assinatura em 2001.[146] O Protocolo 181 visava a aprimorar a aplicação dos princípios consagradas na Convenção 108 adicionando duas novas disposições substantivas. A primeira, requer que os Estados-partes estabeleçam autoridades de supervisão com poderes de investigação e de

[145] CONSELHO DA EUROPA, 1981. p. 4.

[146] CONSELHO DA EUROPA. **Additional protocol to Convention 108 regarding supervisory authorities and transborder data flows (ETS No. 181)**. Estrasburgo, 8 nov. 2001. Disponível em: https://rm.coe.int/1680080626. Acesso em: 2 nov. 2023.

intervenção, que devem ser exercidos com completa independência. A segunda, inclui prescrições para regular as transferências de dados para um país destinatário que não seja parte da Convenção 108.

A esse respeito, o artigo 2º do Protocolo 181 introduziu como critério para as transferências internacionais de dados a garantia de nível de proteção adequada do país destinatário, bem como a possibilidade de realizar transferências caso existam outras formas de garantia ou alternativas, como as cláusulas contratuais, desde que aprovadas pelas autoridades competentes. A transcrição do referido dispositivo[147] segue, abaixo:

> Artigo 2 - Fluxos por sobre fronteiras de dados pessoais para um destinatário que não está sujeito à jurisdição de um Estado-parte da Convenção.
> 1. Cada Estado-parte poderá permitir a transferência de dados pessoais para um destinatário que está sujeito à jurisdição de um Estado ou organização que não seja Parte na Convenção apenas se esse Estado ou organização garantir um nível adequado de proteção para a transferência dos dados pretendida.
> 2. Em derrogação ao parágrafo 1 do Artigo 2 deste Protocolo, cada Estado-parte pode permitir a transferência de dados pessoais:
> a. Se a legislação nacional o permitir devido a:
> - Interesses específicos do titular dos dados, ou
> - Legítimos interesses predominantes, especialmente interesses públicos relevantes, ou
> b. Se garantias, que podem resultar, em particular, de cláusulas contratuais, forem fornecidas pelo controlador responsável pela transferência e forem consideradas adequadas pelas autoridades competentes de acordo com a legislação nacional (tradução livre).

Além do Protocolo 181, a Convenção 108 também passou por um processo mais profundo de modernização, que será tratado a seguir.

1.2.3.3. Convenção 108+ do Conselho da Europa, de 2018

Mais recentemente, a Convenção 108 foi submetida a um processo de modernização por meio do Protocolo de Alteração 223 do Conselho da Europa, que foi aberto à assinatura em 2018.[148] A alteração passou a ser conhecida como Convenção 108+ e a lista de adesões foi sendo acrescida rapidamente pelos Estados-partes.[149] Segundo o

---

147 CONSELHO DA EUROPA, 2001. p. 2.

148 CONSELHO DA EUROPA. Treaty 223: **protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. Estrasburgo, 18 mai. 2018. Disponível em: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1. Acesso em: 2 nov. 2023.

149 CONSELHO DA EUROPA. Chart of signatures and ratifications of Treaty 223: **protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. 2023 Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures. Acesso em: 2 nov. 2023.

relatório explicativo do documento, diante dos novos desafios que afetam os direitos humanos e a liberdades fundamentais, especialmente o uso crescente das TIC, a globalização das operações de tratamento de dados e o aumento contínuo das transferências de dados pessoais, tornou-se evidente a necessidade de modernizar a Convenção 108 e de fortalecer a sua implementação efetiva. Para refletir desenvolvimentos tecnológicos recentes, como a inteligência artificial, a Convenção 108+ incluiu as operações lógicas e/ou aritméticas na definição de tratamento de dados, por exemplo.

Além disso, o artigo 14 da Convenção 108+ abordou de forma mais detalhada o tema das transferências internacionais de dados em relação aos textos de 1981 e de 2001. De acordo com esse dispositivo, quando os dados são transferidos entre Estados-partes, os Estados não podem proibir ou sujeitar a transferência de dados pessoais a uma autorização especial, a menos que haja riscos reais de contornar as regras da Convenção. A exceção também se aplica se os Estados compartilham regras harmonizadas de proteção por meio de uma organização internacional regional.

Quando os dados são transferidos para um destinatário sob jurisdição de um Estado ou organização internacional que não faz parte da Convenção, a transferência só pode ocorrer se um nível de proteção adequado for assegurado, o que pode ser aferido pelo direito do Estado ou organização internacional ou por meio de salvaguardas aprovadas ou aplicáveis “ad hoc” (ou seja, caso a caso) por instrumentos jurídicos obrigatórios adotados pelas partes envolvidas na transferência.

Apesar das prescrições anteriores, um Estado-parte pode permitir a transferência de dados pessoais em situações particulares, como quando o titular dos dados fornecer o seu consentimento. Ainda, cada Estado-parte deve garantir que sua autoridade de supervisão tenha acesso às informações sobre essas transferências e o direito de proibir, suspender ou impor condições às transferências para proteger os direitos e liberdades fundamentais dos titulares de dados pessoais.

Confira-se a redação do referido dispositivo:[150]

> Artigo 14. Fluxos por sobre fronteiras de dados pessoais.
> 1. Um Estado-parte não poderá, apenas com o único propósito de proteger dados pessoais, proibir ou sujeitar a transferência de tais dados a uma autorização especial em relação a um destinatário que seja submetido à jurisdição de outro Estado-parte da presente Convenção. Tal Estado-parte poderá, entretanto, proibir ou limitar a transferência se houver riscos reais e relevantes de que tal transferência seja para outro Estado-parte, seja de outro Estado-parte para outro, não partícipe, possa ocasionar o contorno

[150] CONSELHO DA EUROPA, 2018. p. 10.

> das prescrições da presente Convenção. Um Estado-parte também pode proibir ou limitar tal transferência se estiver submetido a regras harmonizadas de proteção compartilhadas por Estados pertencentes a uma organização internacional de caráter regional.
> 2. Quando o destinatário for submetido à jurisdição de um Estado ou de uma organização internacional que não seja partícipe da presente Convenção, a transferência de dados pessoais somente poderá ocorrer quando um nível adequado de proteção, baseado nas prescrições dessa Convenção, esteja assegurado.
> 3. Um nível adequado de proteção pode ser assegurado:
> a) pelo direito do Estado de uma organização internacional, incluindo-se os tratados e os acordos internacionais; ou
> b) por meio de salvaguardas aprovadas ou aplicáveis "*ad hoc*" – ou seja, somente para o caso específico – fornecidas por instrumentos jurídicos obrigatórios e aplicáveis por força de lei, adotadas e implantadas pelas pessoas envolvidas na transferência e no futuro tratamento dos dados pessoais.
> 4. A despeito da aplicação das prescrições dos parágrafos anteriores, cada Estado-parte pode permitir que a transferência de dados pessoais ocorre se:
> a) o titular dos dados pessoais houver dado consentimento explícito, específico e livre, após ter sido informado dos riscos envolvidos em razão da ausência de salvaguardas adequadas; ou
> b) os interesses particulares do titular de dados pessoais requererem isso, no caso específico; ou
> c) interesses legítimos e predominantes, em particular interesses públicos relevantes, sejam determinados pelo direito aplicável e essa transferência de dados pessoais se constituir como uma medida necessária e proporcional em uma sociedade democrática; ou
> d) isso constituir uma medida necessária e proporcional em uma sociedade democrática para a finalidade da liberdade de expressão.
> 5. Cada Estado-parte deverá garantir que sua autoridade de supervisão, competente nos termos do Artigo 15 desta Convenção, tenha acesso a todas as informações concernentes às transferências de dados referidas no parágrafo 3(b) e, mediante demanda, referidas nos parágrafos 4(b) e 4(c).
> 6. Cada Estado-parte deverá, também, garantir que a sua autoridade de supervisão possua o direito subjetivo de requerer, à pessoa que transfere dados pessoais, a demonstração da efetividade das salvaguardas ou, ainda, a existência de interesses legítimos e predominantes, bem como que a autoridade de supervisão possa, com o fim de proteger os direitos e liberdades fundamentais dos titulares de dados pessoais, proibir, suspender ou submeter a condições determinadas transferências (tradução livre).

Durante a 44ª reunião plenária, realizada em junho de 2023, o Conselho da Europa divulgou o primeiro módulo de cláusulas contratuais modelo para transferências internacionais de dados pessoais entre controladores com base na Convenção 108+. Essas cláusulas serão complementadas futuramente por dois módulos adicionais. Para o Conselho da Europa, cláusulas padronizadas e pré-aprovadas fornecidas em instrumentos juridicamente vinculantes podem contribuir com nível adequado de proteção assegurado pela Convenção 108+, bem como servir como ponte para mecanismos de transferência

semelhantes, favorecendo a convergência em direção a padrões globais de proteção de dados apropriados.[151]

Segundo a declaração do Conselho da Europa, a experiência prática tem revelado que o uso de instrumentos tais como as cláusulas contratuais modelo é considerado uma maneira fácil de transferir dados por sobre as fronteiras, sendo empregado por grande parte do setor privado. As cláusulas do Conselho da Europa requerem aprovação pelas autoridades competentes locais dos Estados-partes para serem transpostas para os conjuntos nacional e regional disponíveis de instrumentos e mecanismos para as transferências internacionais de dados pessoais entre controladores. Nas cláusulas contratuais modelo, a lei aplicável e a autoridade supervisora serão determinadas pelo país de origem do controlador-exportador dos dados, que é signatário da Convenção 108+.

Em vista da importância de manter a consistência entre os seus instrumentos, os pilares de proteção de dados delineados pelas Convenções 108 e 108+ passaram a ser considerados em outros documentos do Conselho Europa, como a Convenção de Budapeste, que será analisada na sequência.

1.2.3.4. Convenção de Budapeste do Conselho da Europa e seus Protocolos Adicionais

O cibercrime é uma ameaça crescente no contexto atual, no qual infratores exploram a vasta rede de conexões e o uso de tecnologias em atividades individuais e empresariais. Embora tenha se intensificado nos últimos anos, o cibercrime não é uma questão recente, tendo sido abordado pelo Conselho da Europa por meio da Convenção sobre Cibercrime, que foi aberta à assinatura em 2001, em Budapeste.[152] A lista de Estados que aderiram à Convenção inclui Argentina, Colômbia e Brasil.[153] Como sugerido pelo nome, a Convenção de Budapeste nasceu com a missão primordial de combater delitos perpetrados por meio da Internet e demais redes de computadores, sendo o primeiro tratado internacional a incentivar a harmonização de leis e regulamentações nacionais, englobando tanto o direito penal substantivo quanto normas processuais

[151] CONSELHO DA EUROPA. **Model Contractual Clauses for the Transfer of Personal Data from Controller to Controller**. 27 jun. 2023. Disponível em: https://www.coe.int/en/web/data-protection/-/model-contractual-clauses-for-the-transfer-of-personal-data. Acesso em: 2 nov. 2023.

[152] CONSELHO DA EUROPA. **Convention on Crybermcrime**. Budapeste, 23 nov. 2001. Disponível em: https://www.coe.int/en/web/cybercrime/the-budapest-convention. Acesso em: 2 nov. 2023.

[153] CONSELHO DA EUROPA. **Who are the Parties to the Budapest Convention?** 2023. Disponível em: https://www.coe.int/en/web/cybercrime/the-budapest-convention. Acesso em: 2 nov. 2023.

relevantes, e a promover a cooperação entre os Estados-parte no controle do cibercrime.[154]

Após a sua ratificação, impõe-se aos Estados-partes a tarefa de estabelecer um arcabouço legal e ferramentas apropriadas para o enfrentamento do cibercrime e a promoção da segurança cibernética.[155] Entre os temas centrais abordados estão as violações de direitos autorais, fraudes relacionadas a computadores, disseminação de pornografia infantil e violação à segurança de redes.[156] A Convenção de Budapeste se distingue pela incorporação de procedimentos para o acesso a informações no âmbito de investigações. A Convenção de Budapeste é acompanhada de dois protocolos adicionais. O Protocolo Adicional nº 189, de 2003, trata de condutas de natureza racistas e xenófobas cometidos através de sistemas computacionais.[157] Protocolo Adicional nº 224, de 2022, que diz respeito às medidas que reforçam a cooperação e a divulgação de provas eletrônicas.[158]

Os desafios que suscitaram a emissão deste último Protocolo referem-se à necessidade de implementar soluções eficazes para obter a divulgação de dados armazenados em múltiplas jurisdições, que são relevantes para investigações no âmbito desse convênio. Nesse sentido, considerando que as investigações frequentemente podem demandar a transferência internacional de dados pessoais e que os Estados-partes podem ser obrigados a assegurar a proteção de tais dados conforme suas legislações nacionais e/ou outros compromissos internacionais, como a Convenção 108 e 108+, o artigo 14 do Protocolo Adicional nº 224 oferece salvaguardas em matéria de proteção dos dados para permitir que os Estados-partes cumpram com esses deveres.

Os Estados-partes deverão considerar que o tratamento de dados pessoais, de acordo com tais salvaguardas, atende aos requisitos do seu quadro jurídico para as transferências internacionais de dados pessoais. As salvaguardas de proteção previstas no Protocolo Adicional nº 224 somente poderão ser substituídas se os Estados-partes

---

[154] CHANG, Lennon YC; GRABOSKY, Peter. The governance of cyberspace. In: DRAHOS, Peter (ed.), **Regulatory theory: foundations and applications**, Canberra: The Australian National University Press, 2017. pp. 533-551. Disponível em: https://library.oapen.org/bitstream/handle/20.500.12657/31596/1/626829.pdf. Acesso em: 2 nov. 2023.

[155] GSTREIN, 2019, p. 84.

[156] GSTREIN, 2019, p. 84.

[157] CONSELHO DA EUROPA. Treaty 189: **First Protocol on Xenophobia and Racism**. Estrasburgo, 2003. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189. Acesso em: 2 nov. 2023.

[158] CONSELHO DA EUROPA. Treaty 224: **Second Additional Protocol on Enhanced co-operation**. Estrasburgo, 12 maio 2022. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224. Acesso em: 2 nov. 2023.

envolvidos na transferência estiverem vinculados a outro acordo internacional que já estabelece um quadro abrangente para a proteção dos dados transferidos em um contexto de prevenção, detecção, investigação e repressão de crimes, e se os Estados-partes concordarem em conduzir a transferência de dados pessoais com base em outros acordos ou arranjos existentes. Ainda, os Estados-partes somente podem suspender as transferências de dados pessoais se houver evidências substanciais de violação sistemática e material das salvaguardas de proteção de dados acordadas no Protocolo ou se uma violação estiver prestes a ocorrer.

A seguir, a transcrição dos trechos pertinentes ao referido dispositivo:[159]

> Artigo 14 – Proteção de dados pessoais
> 1. Âmbito
> a. Salvo disposição em contrário prevista no n.o 1, alíneas b) e c), cada Parte tratará os dados pessoais que recebe ao abrigo do presente Protocolo em conformidade com os n.o 2 a 15 do presente artigo.
> b. Se, no momento da recepção dos dados pessoais ao abrigo do presente Protocolo, tanto a Parte que procede à transferência como a Parte receptora estiverem mutuamente vinculadas por um acordo internacional que estabeleça um quadro abrangente entre essas Partes para a proteção de dados pessoais, aplicável à transferência de dados pessoais para efeitos de prevenção, detecção, investigação e repressão de infrações penais, e que preveja que o tratamento de dados pessoais ao abrigo desse acordo está em conformidade com os requisitos da legislação em matéria de proteção de dados das Partes interessadas, os termos desse acordo serão aplicáveis no caso das medidas abrangidas pelo âmbito desse acordo, aos dados pessoais recebidos ao abrigo do Protocolo em substituição dos n.o 2 a 15, exceto quando o contrário for mutuamente acordado pelas Partes interessadas.
> c. Se a Parte que procede à transferência e a Parte receptora não estiverem mutuamente vinculadas ao abrigo de um acordo descrito no n.o 1, alínea b), poderão determinar mutuamente que a transferência de dados pessoais ao abrigo do presente Protocolo pode ter lugar com base noutros acordos ou convênios entre as Partes interessadas em substituição dos n.o 2 a 15.
> d. Cada Parte considerará que o tratamento de dados pessoais nos termos do n.o 1, alíneas a) e b) cumpre os requisitos do seu quadro jurídico em matéria de proteção de dados pessoais para as transferências internacionais de dados pessoais, não sendo necessária qualquer outra autorização de transferência ao abrigo desse quadro jurídico. Uma Parte só poderá recusar ou impedir transferências de dados para outra Parte ao abrigo do presente Protocolo por razões de proteção de dados: i) nas condições estabelecidas no n.o 15 quando for aplicável o n.o 1, alínea a), ou ii) nos termos de um acordo ou convênio referido no n.o 1, alíneas b) ou c), quando for aplicável um desses números
> [...]
> 15. Consulta e suspensão
> Uma Parte poderá suspender a transferência de dados pessoais para outra Parte se dispuser de provas substanciais de que a outra Parte viola sistemática ou materialmente os termos do presente artigo ou de que está iminente uma violação material. Não deverá suspender as transferências sem um pré-aviso razoável e apenas depois de as Partes interessadas terem iniciado um período razoável de consultas sem chegar a uma resolução. No entanto, uma Parte poderá suspender provisoriamente as transferências em caso de violação sistemática ou material que represente um risco

[159] CONSELHO DA EUROPA, 2022. p. 14.

> significativo e iminente para a vida ou a segurança de uma pessoa singular ou um prejuízo substancial para a sua reputação ou situação económica, devendo, nesse caso, notificar e iniciar imediatamente consultas com a outra Parte. Se a consulta não tiver conduzido a uma resolução, a outra Parte poderá suspender reciprocamente as transferências se dispuser de provas substanciais de que a suspensão pela Parte que suspende era contrária ao disposto no presente número. A Parte que suspende deverá levantar a suspensão logo que a infração que justifica a suspensão tenha sido corrigida; qualquer suspensão recíproca será levantada nesse momento. Os dados pessoais transferidos antes da suspensão continuarão a ser tratados em conformidade com o presente Protocolo (tradução livre).

As Convenções 108 e 108+, bem como a Convenção de Budapeste, juntamente com seus Protocolos Adicionais, demonstram o relevante papel do Conselho da Europa nas discussões sobre transferências internacionais de dados pessoais, que têm buscado avançar para acompanhar os novos desafios tecnológicas. A Convenção de Budapeste, por sua vez, não elimina a importância de que os países estabeleçam balizas em seus quadro legais para proteção de dados em atividades diversas de persecução penal.

1.2.4. Cooperação Econômica Ásia-Pacífico, APEC

A Cooperação Econômica Ásia-Pacífico (APEC) é um bloco regional, estabelecido em 1989, dedicado ao desenvolvimento econômico e à integração entre as suas Economias-membros.[160] A APEC opera por meio de comitês e grupos de trabalho voltados a uma ampla gama de pautas econômicas e comerciais. Conforme será aprofundado adiante, um dos principais temas abordados pela APEC refere-se à proteção de dados, sendo conduzido, sobretudo, pelo *Digital Economy Steering Group* (DESG), antes conhecido como *Electronic Commerce Steering Group* (ECSG), e pelo seu subgrupo *Data Privacy* (DPS).[161]

1.2.4.1. O Marco de Privacidade da APEC

A regulação da proteção de dados no âmbito da APEC se dá por meio do Marco de Privacidade (*Privacy Framework*), instrumento voluntário inaugurado em 2005.[162] Nos termos do preâmbulo, o Marco foi estruturado com base nas Diretrizes de

[160] APEC. **About APEC: History**, out. 2023, Disponível em: https://www.apec.org/about-us/about-apec/history. Acesso em: 2 nov. 2023.

[161] CENTRE FOR INFORMATION POLICY LEADERSHIP. **APEC CBPR & PRP Questions and Answers**, mar. 2020(b). pp. 9. Disponível em: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/03/cipl_cbpr_and_prp_q_a_final__19_march_2020_.pdf. Acesso em: 2 nov. 2023.

[162] APEC. **APEC Privacy Framework**. Asia-Pacific Economic Cooperation. dez. 2005. Disponível em: https://www.apec.org/publications/2005/12/apec-privacy-framework. Acesso em: 2 nov. 2023.

Privacidade da OCDE de 1980, que, naquele momento, refletiam o consenso internacional de práticas para o tratamento de dados pessoais na forma de *soft law*. Em 2015, o modelo foi atualizado, abrangendo conceitos presentes nas Diretrizes de Privacidade da OCDE de 2013 e adaptando-os às diferentes características jurídicas e ao contexto da região da APEC.[163] A aproximação com as Diretrizes de Privacidade da OCDE reflete a intenção de que o Marco de Privacidade da APEC incorpore uma abordagem econômica.[164]

O Marco de Privacidade da APEC é composto por um conjunto de princípios e diretrizes para orientar as Economias-membros a estabelecer medidas de proteção apropriadas contra o uso inadequado de dados pessoais, visando a concretizar os benefícios do comércio eletrônico. Esse modelo concentra-se em assegurar abordagens regulatórias que sejam consistentes em cada Economia-membro, ao invés de idênticas, a fim de conciliar a proteção de dados com os interesses comerciais e a diversidade cultural existente entre os seus membros. O Marco de Privacidade da APEC destaca a importância da livre circulação de dados e busca evitar a imposição de obstáculos às transferências de dados na região.

1.2.4.2. *Cross-Border Privacy Rules* e *Privacy Recognition for Processors,* APEC

Em 2011, a APEC instituiu o sistema de *Cross-Border Privacy Rules* (CBPR), que constitui um mecanismo para as transferências internacionais de dados pessoais na forma de um esquema de certificação voluntário, cujo foco da proteção reside na responsabilidade dos agentes envolvidos (*accountability*), em vez do local onde os dados são tratados.[165] Nesse sentido, o sistema CBPR pode ser usado, por exemplo, em transferências para empresas do mesmo grupo econômico, para empresas independentes e também para empresas não certificadas pelo CBPR em qualquer parte do mundo, desde que o agente que irá transferir os dados esteja sob a jurisdição de uma autoridade de supervisão (em inglês, *Privacy Enforcement Authority* ou PEA) na Economia-membro da APEC na qual se busca a certificação.[166] O sistema CBPR foi integralmente

[163] APEC. **APEC Privacy Framework.** Asia-Pacific Economic Cooperation, 2015. Disponível em: https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015). Acesso em: 2 nov. 2023.
[164] CHANDER; SCHWARTZ, 2023. 88.
[165] APEC. **APEC Cross-Border Privacy Rules (CBPR) System**. 2023(b). Disponível em: https://cbprs.org. Acesso em: 2 nov. 2023.
[166] CIPL, 2020(b). p. 3.

implementado em Economias-membros da APEC como os EUA, Japão, Coreia do Sul e Singapura.

Os agentes que optarem por aderir ao sistema CBPR devem estabelecer políticas e práticas de proteção de dados em consonância com os requisitos do programa CBPR que compreendam os dados pessoais sujeitos à transferência. Tais requisitos buscam operacionalizar os princípios previstos no Marco de Privacidade da APEC. O sistema CBPR igualmente requer a incorporação de proteções baseadas em risco, incluindo salvaguardas de segurança para dados pessoais proporcionais à probabilidade e gravidade do risco, à natureza ou sensibilidade dos dados e ao contexto em que são mantidos.[167] A certificação é conduzida por uma entidade terceirizada aprovada em uma Economia-membro da APEC, conhecida como Agente de Responsabilidade (em inglês, *Accountability Agent*).[168] Um traço distintivo do sistema CBPR é que as entidades certificadoras podem ter natureza privada.

Os agentes interessados em obter a certificação CBPR devem submeter uma aplicação ao Agente de Responsabilidade aprovado na Economia-membro na qual está primordialmente localizado, acompanhada de uma autoavaliação sobre as suas políticas e práticas de proteção de dados. Durante o processo de certificação, o Agente de Responsabilidade utiliza um conjunto de critérios específicos associados a cada um dos requisitos do programa CBPR para avaliar a conformidade das políticas e práticas de proteção de dados do candidato.

Uma vez que o agente tenha sido certificado para participar do sistema CBPR, a observância das políticas e práticas de proteção de dados se torna uma obrigação vinculante e poderá ser executada por uma autoridade de supervisão/PEA na Economia-membro em que o agente foi certificado. Cabe destacar que essas autoridades devem fazer parte do Acordo de Execução de Privacidade Transfronteiriça da APEC (em inglês, *Cross-border Privacy Enforcement Arrangement* ou CPEA), um mecanismo multilateral que permite que as autoridades cooperem na execução da proteção de dados por meio do compartilhamento de informações e de outras medidas de assistência mútua.[169]

---

[167] APEC. **What is the Cross-Border Privacy Rules System**, jun. 2023(c). Disponível em: https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system#:~:text=The%20APEC%20Cross%2DBorder%20Privacy,internationally%2Drecognized%20data%20privacy%20protections. Acesso em: 2 nov. 2023.

[168] APEC. **APEC Cross-Border Privacy Rules System Policies, Rules and Guidelines**. 2011. Disponível em: http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_desarrollos_APEC_3.pdf. Acesso em: 2 nov. 2023.

[169] APEC, 2023.

Mais tarde, em 2015, a APEC desenvolveu o *Privacy Recognition for Processors* (PRP), uma certificação complementar ao sistema CBPR voltada para operadores de dados que tratam dados pessoais em nome dos controladores. Os requisitos do programa PRP são mais enxutos, concentrando-se principalmente na segurança dos dados e na capacidade de implementar os requisitos relevantes do CBPR e as instruções de proteção de dados do controlador. O objetivo principal do PRP é servir como uma ferramenta de diligência para identificar operadores qualificados. As etapas do processo de certificação do PRP são similares às da CBPR. [170]

Vale notar que os sistemas CBPR e PRP não substituem as legislações nacionais e não isentam empresas ou reguladores de suas responsabilidades em relação à proteção de dados. A adoção desses sistemas depende da sua compatibilidade com as normas locais de proteção de dados.[171]

1.2.5. Fórum Global *Cross-Border Privacy Rules*

Em 2022, EUA, Canadá, Japão, Singapura, Filipinas, Coreia do Sul e Taipé Chinesa publicaram uma declaração para instaurar o Fórum Global *Cross-Border Privacy Rules* (Fórum Global CBPR), que se propõe a estabelecer um sistema de certificação internacional baseado nos já existentes sistemas CBPR e PRP, expandindo a participação de países que não integram as Economias-membros da APEC.[172] O referido sistema global busca apoiar a livre circulação de dados e, ao mesmo tempo, a proteção da privacidade e dos dados pessoais.

Conforme delineado na declaração, sua intenção é ser aberto a todos os países que aceitarem os objetivos e princípios do Fórum Global CBPR. O sistema CBPR do Fórum Global é independente e separado dos atuais sistemas CBPR e PRP da APEC. Todos os Agentes de Responsabilidade aprovados e as empresas certificadas foram automaticamente reconhecidos no novo sistema CBPR do Fórum Global com base nos mesmos termos em que são reconhecidos nos sistemas CBPR e PRP da APEC.[173]

---

[170] APEC. **APEC Privacy Recognition for Processors ("PRP") Purpose and Background**. 28 ago. 2015. Disponível em: http://cbprs.org/wp-content/uploads/2020/08/PRP-Purpose-and-Background-4.pdf. Acesso em: 2 nov. 2023.

[171] REMOLINA, 2015, pp. 194-195.

[172] GLOBAL CBPR FORUM. **Global Cross-Border Privacy Rules (CBPR) Declaration**. 21 abr. 2022. p. 2. Disponível em: https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-Declaration-2022.pdf. Acesso em: 2 nov. 2023.

[173] GLOBAL CBPR FORUM. **About the Global CBPR Forum**. 2023. https://www.globalcbpr.org/about/. Acesso em: 2 nov. 2023.

Durante o seu primeiro ano, os membros focaram em três objetivos principais. Primeiro, estabelecer a estrutura inicial de governança do Fórum e procedimentos. Segundo, definir critérios e procedimentos para adesão e participação no Fórum. Terceiro, promover o Fórum para jurisdições e partes interessadas.[174] Em 2023, o Fórum emitiu um conjunto de documentos, incluindo o Marco Global CBPR, que foi inspirado no Marco de Privacidade da APEC.[175] Esse movimento reitera o objetivo de estabelecer padrões interoperáveis de proteção de dados em diferentes jurisdições que não sejam necessariamente idênticos. Atualmente, o Fórum está trabalhando ativamente para operacionalizar o seu novo sistema, convidando jurisdições fora da APEC para participar do processo, o que poderá ter um impacto significativo para os fluxos de dados ao redor do mundo.

1.2.6. Rede Ibero-americana de Proteção de Dados, RIPD

A Rede Ibero-americana de Proteção de Dados (RIPD) foi fundada em 2003 e constituí um fórum regional que integra diversos atores, tanto do setor público como do setor privado, incluindo autoridades nacionais de proteção de dados, entre as quais se encontram as autoridades da Argentina, do Uruguai, da Colômbia e do Brasil.[176] A participação de organizações da sociedade civil nas atividades e eventos da RIPD ocorre por meio do Fórum da Sociedade Civil. A RIPD desenvolve iniciativas e projetos voltados à proteção de dados no espaço ibero-americano, com o intuito de manter e fortalecer o intercâmbio de informação, experiências e conhecimentos. Esse movimento considera a necessidade de um fluxo de dados contínuo entre países ibero-americanos com laços comuns e preocupação compartilhadas na temática de proteção de dados.[177]

O propósito de estabelecer a RIPD foi declarado durante o I Encontro Ibero-americano de Proteção de Dados (EIPD) em 2002, na Espanha. Já no ano subsequente, em Antígua, Guatemala, durante o II EIPD, a RIPD foi formalmente instituída. O

---

[174] GLOBAL CBPR FORUM. **Global Forum Assembly, Annual Work Program, through April 2024.** 30 jun. 2023**.** Disponível em: https://www.globalcbpr.org/the-forum-releases-its-annual-work-program-for-2023-2024/. Acesso em: 2 nov. 2023.

[175] GLOBAL CBPR FORUM. **Global Cross-Border Privacy Rules (CBPR) Framework (2023)**. 2023. Disponível em: https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-Framework-2023.pdf. Acesso em: 2 nov. 2023.

[176] REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. **Relación de entidades integrantes de la RIPD**. 2023. Disponível em: https://www.redipd.org/es/la-red/entidades-acreditadas. Acesso em: 2 nov. 2023.

[177] REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. **Historia de la Red Iberoamericana de Protección de Datos (RIPD)**. 2023. Disponível em: https://www.redipd.org/es/la-red/historia-de-la-red-iberoamericana-de-proteccion-de-datos-ripd. Acesso em: 2 nov. 2023.

resultado foi reforçado na Declaração Final da XIII Cúpula dos Chefes de Estado e Governo dos países Ibero-americanos.[178] Os objetivos e a organização da RIPD estão contidos no Regulamento aprovado no VI EIPD, realizado em 2008, e revisado no XVI EIPD, em 2018.[179] Desde a sua concepção, a RIPD reconhece a proteção de dados pessoais como um direito fundamental, bem como a importância de iniciativas regulatórias no espaço ibero-americanas para essa proteção.[180]

1.2.6.1. Padrões de Proteção de Dados dos Estados Ibero-Americanos

Um marco significativo para a RIPD ocorreu durante o XVI EIPD, em 2017, com a aprovação dos Padrões de Proteção de Dados Pessoais para os Estados Ibero-americanos. Os Padrões Ibero-americanos estabelecem um conjunto de diretrizes orientadoras, que contribuem para impulsionar a regulação da proteção de dados pessoais na região ibero-americana, seja como motor de iniciativas legislativos em países que ainda não contam com marcos jurídicos no tema, seja como referência para modernização e atualização das legislações já existentes.[181]

Como precursor direto desses Padrões, cita-se a implementação pela RIPD, em 2007, durante o V EIPD, das Diretrizes para a Harmonização da Proteção de Dados na Comunidade Ibero-americana. O objetivo dessas diretrizes era criar um quadro harmonizado como referência para possíveis iniciativas regulatórias nacionais relacionadas à proteção de dados na região. Além disso, na elaboração dos Padrões Ibero-Americanos, também foram observados outros instrumentos internacionais, que incluem as Diretrizes de Privacidade da OCDE, a Convenção 108 do Conselho da Europa e o Marco de Privacidade da APEC.

Entre os objetivos dos Padrões Ibero-americanos, destaca-se o estabelecimento de um conjunto de princípios e direitos comuns para proteção de dados

---

178 CUMBRE IBEROAMERICANA. **XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno 14 y 15 de Noviembre**. Santa Cruz de la Sierra, 2003. p. 11. Disponível em: https://www.segib.org/wp-content/uploads/DeclaraciondeSantaCruz.pdf. Acesso em: 2 nov. 2023.

179 REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. **Regulamento da Rede Ibero-Americana de Proteção de Dados (RIPD)**. 2018. p. 10. Disponível em: https://www.redipd.org/sites/default/files/inline-files/REGLAMENTO_RIPD_REV30_11_18_PT.pdf. Acesso em: 2 nov. 2023.

180 REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. **Historia de la Red Iberoamericana de Protección de Datos (RIPD)**. 2023. Disponível em: https://www.redipd.org/es/la-red/historia-de-la-red-iberoamericana-de-proteccion-de-datos-ripd. Acesso em: 2 nov. 2023.

181 REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. **Padrões de Proteção de Dados Pessoais para os Estados Ibero-Americanos**. 20 jun. 2017. pp. 34. Disponível em: https://www.redipd.org/sites/default/files/inline-files/Estandares_PORTUGUES.pdf. Acesso em: 2 nov. 2023.

pessoais, que os Estados Ibero-americanos podem adotar e desenvolver em suas respectivas legislações nacionais, a fim de contar com regras homogêneas na região, além da garantia do efetivo exercício e tutela do direito à proteção de dados pessoais de qualquer pessoa física nos Estados Ibero-americanos, mediante a determinação de regras comuns que assegurem o devido tratamento de seus dados pessoais. Ainda, os objetivos incluem facilitar o fluxo de dados entre os Estados Ibero-americanos e fora de suas fronteiras, com o propósito de colaborar para o crescimento econômico e social da região, e encorajar a cooperação internacional entre as autoridades de supervisão dos Estados Ibero-americanos com outras autoridades não pertencentes à região, e com organizações internacionais na matéria.

O artigo 36 dos Padrões Ibero-americanos disciplina as transferências internacionais de dados pessoais. Nos termos desse dispositivo, os agentes podem realizar a transferência quando o país ou organização destinatária apresentar um nível adequado de proteção, conforme a legislação do Estado de origem. Alternativamente, o agente que envia os dados deve fornecer garantias adequadas acerca do tratamento de dados no país destinatário, que deve respeitar padrões mínimos estabelecidos pelos Estados Ibero-americanos.

As cláusulas contratuais firmadas entre os agentes envolvidos também podem ser usadas como garantia de tratamento adequado, que podem ser validadas pelas autoridades de supervisão correspondentes. Além disso, mecanismos de autorregulação ou certificação aprovados podem ser adotados. A autoridade de supervisão do Estado de origem pode, ainda, autorizar a transferência, conforme a legislação local. Admite-se que as leis nacionais dos Estados Ibero-americanos limitem as transferências de dados por razões de segurança, saúde pública, direitos de terceiros ou interesse público.

Confira-se a redação do referido dispositivo:[182]

> Transferências internacionais de dados pessoais
> 36. Regras gerais para transferências de dados pessoais
> 36.1. O controlador e o operador poderão realizar transferências internacionais de dados pessoais em quaisquer dos seguintes casos:
> a. O país, parte de seu território, setor, atividade ou organização internacional destinatária dos dados pessoais tiver sido reconhecido com nível adequado de proteção de dados pessoais pelo país que realiza a transferência, conforme a legislação nacional desse que resultar aplicável na matéria, ou então, o país destinatário ou vários setores dele consignarem condições mínimas e suficientes para garantir um adequado nível de proteção dos dados pessoais.
> b. O exportador ofereça garantias suficientes do tratamento dos dados pessoais no país destinatário, e este, por sua vez, acreditar o cumprimento

[182] REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS, 2017. p. 29.

> das condições mínimas e suficientes estabelecidas na legislação nacional de cada Estado Ibero-Americano aplicável na matéria.
> c. Exportador e destinatário subscreverem cláusulas contratuais ou qualquer outro instrumento jurídico que ofereça garantias suficientes e que permita demonstrar o alcance do tratamento dos dados pessoais, das obrigações e responsabilidades assumidas pelas partes e dos direitos dos titulares. A autoridade de controle poderá validar cláusulas contratuais ou instrumentos jurídicos segundo determinar na legislação nacional dos Estados Ibero-americanos aplicável na matéria.
> d. Exportador e destinatário adotarem um esquema de autorregulação vinculante ou mecanismo de certificação aprovado, sempre que seja conforme as disposições previstas na legislação nacional do Estado Ibero-americano aplicável na matéria, que o exportador estará obrigado a observar.
> e. A autoridade de controle do Estado Ibero-americano do país do exportador autorizar a transferência, em termos da legislação nacional que for aplicável na matéria.
> 36.2. A legislação nacional dos Estados Ibero-americanos aplicável na matéria poderá estabelecer expressamente limites às transferências internacionais de categorias de dados pessoais por razões de segurança, segurança pública, proteção à saúde pública, proteção dos direitos e liberdades de terceiros, bem como questões de interesse público.

À luz dos Padrões Ibero-americanos acima, que estabelecem que o uso de cláusulas contratuais constitui uma alternativa para realizar transferências internacionais de dados pessoais, a RIPD trabalhou na elaboração de um modelo para a região, como será tratado a seguir.

1.2.6.2. Cláusulas Contratuais Modelo da RIPD

Em 2021, a RIPD lançou as suas cláusulas contratuais modelo em duas versões, uma para transferências entre controladores e outra para transferências de controladores para operadores.[183] Até então, não havia cláusulas dessa natureza aprovadas de forma conjunta no âmbito da América Latina. Segundo a RIPD, as versões propostas representam o primeiro passo e espera-se que, no futuro, sejam desenvolvidos módulos adicionais para transferências entre operadores e de operadores para controladores. As cláusulas contratuais modelo propostas pela RIPD contêm, em sua essência, elementos e princípios básicos para garantir transferências seguras.

Juntamente com elas, a RIPD lançou o Guia para a Implementação de Cláusulas Contratuais Modelo para a Transferência Internacional de Dados Pessoais, que busca esclarecer os principais aspectos que devem ser considerados quando as

[183] REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. **Modelos de Cláusulas Contratuais**. 2021. p. 47. Disponível em: https://www.redipd.org/sites/default/files/2023-02/anexo-modelos-clausulas-contractuales-pt.pdf. Acesso em: 2 nov. 2023.

transferências internacionais são realizadas com base nesse mecanismo.[184] Para a RIPD, as cláusulas contratuais modelo contribuem para construir a convergência em nível contratual, criando um regime autônomo de proteção de dados, sem necessariamente exigir convergência em nível de país. Nesse sentido, a RIPD assinala que as cláusulas contratuais modelo constituem uma solução econômica para o desafio das transferências internacionais, pois os agentes não precisam contar com profissionais para elaborar e negociar contratos, o que implica em custos legais e de tempo. A pré-aprovação de cláusulas pela RIPD, assim, objetiva oferecer uma solução prática e simples, especialmente benéfica para pequenas e médias empresas.[185]

Além disso, as cláusulas contratuais modelo estipulam que as partes devem ser capazes de comprovar o seu cumprimento, o que requer a responsabilidade e prestação de contas pelos agentes envolvidos na transferência. Em particular, é exigido que o agente receptor dos dados mantenha documentação relativa às atividades de tratamento e informe se, por algum motivo, não puder cumprir com as cláusulas estabelecidas.[186] Cabe destacar que o referido Guia não substitui os regulamentos e diretrizes emitidos pelas autoridades de supervisão dos Estados Ibero-americanos. Se houver contradição entre o Guia e as orientações das autoridades nacionais de supervisão, recomenda-se seguir as orientações das autoridades, visto que cabe a elas definir as regras para a realização de transferências internacionais de dados pessoais conforme a legislação local.[187]

Com base nessas iniciativas, observa-se que a RIPD, no decorrer do tempo, tem se consolidado na região latino-americana como um fórum destacado e realizou avanços nas discussões das transferências internacionais de dados pessoais.

1.2.7. Mercosul

O Mercado Comum do Sul (Mercosul) é um bloco econômico e político instituído em 1991 na região sul-americana pelo Tratado de Assunção.[188] Seus membros

---

[184] REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. **Guia para a Implementação de Cláusulas Contratuais Modelo para a Transferência Internacional de Dados Pessoais (TIDP).** 2021. Disponível em: https://www.redipd.org/sites/default/files/2023-02/guia-implementacion-clausulas-contractuales-modelo-tidp-pt.pdf. Acesso em: 2 nov. 2023.

[185] REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS, 2021. pp. 16-18.

[186] REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS, 2021. pp. 23-24.

[187] REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS, 2021. pp. 3-5.

[188] MERCOSUL. **Tratado de Assunção para a Constituição de um Mercado Comum**. Assunção, 1991. p.30. Disponível em: https://www.mercosur.int/documento/tratado-de-assuncao-para-a-constituicao-de-um-mercado-comum/. Acesso em: 2 nov. 2023..

fundadores são Brasil, Argentina, Paraguai e Uruguai, denominados de Estados-partes.[189] Em 2012, a Venezuela foi integrada aos Estados-partes, contudo, em 2016, foi suspensa por violação aos compromissos estabelecidos pelo Mercosul.[190] Entre os objetivos do Mercosul estão a livre circulação de bens, serviços e fatores produtivos, bem como o compromisso dos Estados-partes de harmonizar suas legislações, nas áreas pertinentes, para lograr o fortalecimento do processo de integração.[191]

O Tratado de Assunção está aberto à adesão de novos membros provenientes da Associação Latino-Americana de Integração, o que indica uma projeção de crescimento do Mercosul na América do Sul. Como resultado dessa projeção, a Bolívia caminha para se consolidar como um Estado-parte do bloco. Além disso, alguns países têm o reconhecimento de Estado Associado, como é o caso da Colômbia, o que lhes permite participar de atividades e reuniões do bloco.[192]

1.2.7.1. Acordo sobre Comércio Eletrônico do Mercosul

Embora a discussão sobre a proteção de dados no Mercosul já ocorra há algum tempo,[193] com a assinatura do Acordo sobre Comércio Eletrônico, em 28 de janeiro de 2021, foram estabelecidas, pela primeira vez, normas de proteção de dados em nível regional cujo cumprimento é obrigatórias para todos os Estados-partes.[194]O Acordo foi formalizado por meio da Decisão nº 15/20 do Conselho do Mercado Comum (CMC), órgão superior do Mercosul, responsável por conduzir o processo de integração e tomar decisões para garantir o cumprimento dos objetivos estabelecidos pelo Tratado de Assunção.[195]

---

[189] MERCOSUL. **Países do MERCOSUL**. 2023. Disponível em: https://www.mercosur.int/pt-br/quem-somos/paises-do-mercosul/. Acesso em: 2 nov. 2023.

[190] MERCOSUL. **Decisão sobre a suspensão da Venezuela no MERCOSUL**. 5 ago. 2017. Disponível em: https://www.mercosur.int/pt-br/decisao-sobre-a-suspensao-da-republica-bolivariana-da-venezuela-no-mercosul/. Acesso em: 2 nov. 2023.

[191] MERCOSUL. **Objetivos do MERCOSUL**. 2023. Disponível em: https://www.mercosur.int/pt-br/quem-somos/objetivos-do-mercosul/. Acesso em: 2 nov. 2023.

[192] MERCOSUL. **Países do MERCOSUL**. 2023. Disponível em: https://www.mercosur.int/pt-br/quem-somos/paises-do-mercosul/. Acesso em: 2 nov. 2023.

[193] DELPIAZZO, Carlos E.; PASCALE, Maricarmen; PEÑA, Daniela; MELERAS, Flavia; SARAVIA. Andrés. **Protección de datos personales en Uruguay y el Mercosur**. Montevidéu: Fundación de Cultura Universitaria, 2005.

[194] MERCOSUL. **Decisão nº 15/20: Acordo sobre Comércio Eletrônico do Mercosul**. Conselho do Mercado Comum (CMC). 29 abr. 2021. p. 9. Disponível em: https://www.mercosur.int/documento/acordo-sobre-o-comercio-eletronico-do-mercosul/. Acesso em: 2 nov. 2023.

[195] VIOLA, Mario; FRANCA, Marcílio; DONEDA, Danilo. **Festa para a proteção de dados na América do Sul**. ConJur, 17 fev. 2021. Disponível em: https://www.conjur.com.br/2021-fev-17/opiniao-festa-protecao-dados-america-sul. Acesso em: 2 nov. 2023.

O artigo 6.2 do referido Acordo prevê que os Estados-partes devem adotar ou manter leis, regulamentos ou medidas administrativas para a proteção dos dados pessoais dos usuários envolvidos no comércio eletrônico. Para tais fins, devem considerar os padrões internacionais existentes na matéria e envidar esforços para assegurar que os seus marcos jurídicos para a proteção dos dados pessoais dos usuários do comércio eletrônico não sejam aplicados de forma discriminatória. Ainda, pelo artigo 6.7 do Acordo, é previsto que os Estados-partes se comprometam a aplicar um nível adequado de proteção aos dados pessoais que recebem de outro Estado-parte mediante uma norma geral ou autônoma específica ou por acordos mútuos, gerais ou específicos, ou em marcos internacionais mais amplos, admitindo para o setor privado a implementação de contratos ou de autorregulação.

O Acordo também se refere ao estabelecimento de medidas comuns de proteção de dados nas transferências internacionais de informações por meios eletrônicos. O artigo 7º do Acordo estabelece que cada Estado-parte poderá ter seus próprios requisitos regulatórios sobre a transferência de informação por meios eletrônicos, inclusive com relação à proteção de dados pessoais. Ainda, cada Estado-parte deverá permitir a transferência internacional de informações por meios eletrônicos, quando essa atividade tiver por objetivo a realização da atividade comercial de pessoas de um outro Estado-parte, que deve aplicar nível adequado de proteção, nos termos do artigo 6.7, Por fim, os Estados-partes podem adotar ou manter medidas que obstem as transferências internacionais de dados para alcançar objetivos legítimos de políticas públicas, desde que a medida não seja aplicada de maneira que constitua um meio de discriminação arbitrária ou injustificada ou uma restrição encoberta ao comércio eletrônico. O Acordo ressalva que essas prescrições não se aplicam aos serviços financeiros.

Ao reconhecer a proteção de dados pessoais no âmbito do comércio eletrônico, inclusive para a melhoria da confiança dos usuários nas transferências internacionais de dados pessoais, o Acordo, portanto, reflete que o Mercosul tem buscado avançar na promoção de padrões comuns e maior integração do tema no bloco.

1.3. Conclusão do Capítulo

Neste Capítulo, foi possível observar que os dados pessoais, as TIC e a Internet são componentes-chave para a evolução das transferências internacionais de dados pessoais. À medida que dados pessoais assumiram relevância social, econômica e

política e se tornaram amplamente disponíveis por meio das TIC, a Internet é a principal rede que promove a sua transferência por sobre as fronteiras. Nesse contexto interconectado, a partir das contribuições das teorias de regulação da Internet, observa-se que regimes para a tutela das transferências internacionais de dados pessoais podem alcançar maior interoperabilidade jurídica com base em modelos regulatórios híbridos, em que há a distribuição de responsabilidades entre os diversos atores envolvidos no processo regulatório. Esses modelos podem incluir instrumentos e estratégias regulatórias que contemplem a proteção de dados na arquitetura, a responsabilização e prestação de contas dos agentes (*accountability*) e avaliações para o dimensionamento dos riscos associados às transferências.

Tais aspectos podem ser observados nos instrumentos internacionais e regionais analisados neste Capítulo, que buscam construir padrões comuns de conformidade jurídica para a proteção de dados. Conforme examinado, desde os anos 70 tem havido um movimento que resultou na formação de redes internacionais e regionais para a troca de conceitos e práticas voltadas à proteção de dados, que foi motivado, entre outras razões, para possibilitar os fluxos de dados. Os esforços iniciais foram fundamentais para estabelecer um conjunto comum de princípios a serem aplicados na proteção de dados, conhecido como *Fair Information Principles*. De maneira progressiva, organizações como a OCDE e o Conselho da Europa assumiram a liderança dessas iniciativas. Com o passar dos anos, essa tendência se expandiu para outras regiões, incluindo a APEC, a RIPD e, mais recentemente, encontrou expressão no contexto de comércio eletrônico do Mercosul.

Os instrumentos originados desse processo têm desempenhado um papel importante para a consolidação de padrões comuns no tema, como é o caso das Diretrizes de Privacidade da OCDE, as Convenções 108 e 108+ e a Convenção de Budapeste do Conselho da Europa, o Marco de Privacidade e o sistema CBPR da APEC, os Padrões Ibero-americanos da RIPD e o Acordo sobre Comércio Eletrônico do Mercosul. A despeito das diferenças relacionadas à sua natureza e efeitos jurídicos, esses instrumentos refletem a importância da interconexão jurídica em matéria de proteção de dados e conduzem à conclusão de que inciativas isoladas para regular a proteção de dados possuem eficácia limitada.

Nesse sentido, é evidente o empenho para eliminar barreiras injustificadas que possam impedir os fluxo de dados entre os países aderentes a instrumentos como as Diretrizes de Privacidade da OCDE, as Convenções 108 e 108+ do Conselho da Europa,

e o Acordo sobre Comércio Eletrônico do Mercosul, e que eventuais restrições devem ser justificadas e ponderadas. Percebe-se que também foram integradas abordagens híbridas para autorizar as transferências internacionais de dados pessoais. Elas incluem a avaliação do quadro legal de proteção de dados do país destinatário dos dados, bem como a implementação de medidas organizacionais, pelos agentes envolvidos na transferência associadas à responsabilidade e prestação de contas e à avaliação de riscos das transferências. Dentre essas medidas, destacam-se mecanismos voluntários, como o estabelecimento de cláusulas contratuais e de outros meios de autorregulação vinculante que ofereçam garantias suficientes de proteção. Os mecanismos voluntários refletem meios para facilitar a adesão de padrões de proteção de dados de sistemas jurídicos distintos. Importa frisar o sistema de certificação do Fórum Global CBPR, que tem o potencial de se expandir globalmente e de trazer um novo cenário para os fluxos de dados entre países.

Cabe notar que os instrumentos internacionais e regionais alinhados à tradição jurídica europeia, como a Convenções do Conselho da Europa e os Padrões Ibero-americanos da RIPD, oferecem abordagens segundo a ótica dos direitos fundamentais. Por outro lado, os instrumentos orientados sob a ótica comercial, como os documentos da OCDE e da APEC, têm como foco os benefícios decorrentes do comércio internacional e eletrônico. O destaque dessas nuances é importante para a análise do Capítulo seguinte, que se inicia com o estudo das diferentes construções jurídicas de proteção de dados da UE e dos EUA.

2. DE PRINCÍPIOS BÁSICOS, INSTRUMENTOS INTERNACIONAIS E REGIONAIS PARA MODELOS JURÍDICOS DE PROTEÇÃO DE DADOS

2.1. As diferentes construções jurídicas da UE e dos EUA em matéria de proteção de dados

Os instrumentos internacionais e regionais analisados anteriormente impulsionaram uma base comum em torno de princípios básicos e padrões comuns para os modelos de proteção de dados ao redor do mundo. No entanto, particularidades culturais, históricas e jurídicas específicas de cada região podem levar a variações significativas na implementação de aspectos regulatórios.[196] Assim, diante das variadas construções jurídicas de proteção de dados presentes no cenário global, é possível destacar a existência de dois modelos regulatórios com marcantes diferenças: o modelo da UE e o modelo dos EUA.[197]

Como será aprofundado nesta Seção, as diferenças entre os modelos jurídicos de proteção de dados da UE e dos EUA estão associadas a três fatores principais. O primeiro refere-se a como cada um concebe a proteção de dados. O segundo diz respeito à existência ou ausência de normas gerais para regular o tratamento de dados pessoais. O terceiro, por fim, trata da implementação de APD para supervisionar as normas.[198] No decorrer do tempo, as distintas abordagens também têm impactado as transferências transatlânticas de dados pessoais. Enquanto a UE tem buscado aplicar regimes estritos acerca das transferências de dados pessoais para países terceiros que não tenham um nível adequado de proteção, os EUA acabaram por não consolidar uma regulação estrita, o que será examinado adiante.

2.1.1. O modelo jurídico de proteção de dados da UE

No modelo da UE, a proteção de dados é orientada sob a ótica de direitos fundamentais. Os principais documentos que reconhecem expressamente o status constitucional da proteção de dados como um direito fundamental são a Carta de Direitos Fundamentais da UE[199] que se tornou juridicamente obrigatória para seus Estados-membros após a assinatura do Tratado de Lisboa em 2009, e o Tratado sobre o

---

196 KUNER, 2010. p. 35.

197 SCHWARTZ, Paul M. The EU-US privacy collision: a turn to institutions and procedures. **Harvard Law Review,** v. 126, 2012. p. 1966.

198 REMOLINA, 2015. p. 276.

199 UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia** (2000/C 364/01). Bruxelas, 18 dez. 2000. pp. 22. Disponível em: http://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 2 nov. 2023.

Funcionamento da União Europeia.[200-201] De acordo com o direito constitucional europeu, o tratamento adequado de dados pessoais requer uma base normativa. Segundo Christopher Kuner, esse enquadramento traz implicações relevantes, uma vez que sugere que tais normativas sejam resistentes a alterações e que a importância atribuída aos direitos dos titulares é elevada.[202]

Ao longo dos anos, a UE desenvolveu um robusto sistema de proteção administrativo de dados pessoais entre seus Estados-membros. Enquanto alguns dos Estados-membros já possuíam textos legais desde a década de 1970, outros iniciaram seus processos legislativos a partir da transposição da Diretiva de Proteção de Dados 95/46/CE.[203] Esse documento foi projetado para ter aplicação abrangente, cobrindo atividades de tratamento de dados, tanto no setor público quanto no privado. Além disso, a Diretiva 95/46/CE visava à promoção do livre fluxo de informações entre os seus Estados-membros como parte da estratégia para criar um mercado interno de dados pessoais, facilitando a livre circulação de bens, pessoas, serviços e capitais. A manutenção de padrões elevados de proteção de dados para resguardar os direitos dos titulares e a sua uniformidade nos Estados-membros seria essencial para eliminar barreiras ao fluxo de dados, um elemento importante para o funcionamento eficiente do mercado da UE.[204]

Mais tarde, a Diretiva 95/46/CE foi substituída com a promulgação do Regulamento Geral sobre a Proteção de Dados (RGPD) em 2016, que entrou em vigor em 2018.[205] Para Paul M. Schwartz e Karl-Nikolaus Peifer, a substituição de uma diretiva por um regulamento amplia a proteção de dados na União Europeia reafirma a importância atribuída aos titulares dos dados.[206] Isso porque as diretivas não são diretamente vinculantes e exigem a instituição de leis nacionais pelos Estados-membros

---

[200] UNIÃO EUROPEIA. **Tratado sobre o Funcionamento da União Europeia** (2016/C 202/01). EUR-Lex, 7 jun. 2016. pp. 154. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF. Acesso em: 2 nov. 2023.

[201] CHANDER; SCHWARTZ, 2023. p. 90.

[202] KUNER, 2010. p. 27.

[203] 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**. Bruxelas, 24 out. 1995, Disponível em: http://data.europa.eu/eli/dir/1995/46/oj. Acesso em: 2 nov. 2023.

[204] REIGADA, 2012. pp. 22-23.

[205] 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)**. Bruxelas, 27 abr. 2016. Disponível em: http://data.europa.eu/eli/reg/2016/679/oj. Acesso em: 2 nov. 2023.

[206] SCHWARTZ, Paul M.; PEIFER, Karl-Nikolaus. Transatlantic data privacy law. **Georgetown Law Journal**, v. 106, n. 1, p. 115-179, 7 nov. 2017. pp. 128-129.

para refletir as suas prescrições. Em contrapartida, os regulamentos são diretamente aplicáveis à ordem jurídica interna dos Estados-membros, evitando margens de adaptação e propiciando um ambiente regulatório mais uniforme.[207]

O RGPD marca uma distinção na forma como a proteção de dados e a defesa do consumidor são abordadas na UE. Tradicionalmente, a defesa do consumidor no contexto europeu baseia-se no estabelecimento de diretivas, não de regulamentos, e tem uma conexão menos evidente com os direitos fundamentais.[208] A Carta dos Direitos Fundamentais da União Europeia é fundamentada primordialmente pelas seguintes lógicas: empoderar os consumidores, equipando-os com direitos para que possam fazer escolhas informados, e protegê-los em situações de desequilíbrio de poder nas transações comerciais. Assim, as normas da UE relacionadas a esse tema têm como foco as interações comerciais entre consumidores e empresas, de modo a definir regras justas para as transações comerciais.[209]

Com base no RGPD, o modelo europeu de proteção de dados apoia-se em três pilares, que incluem as obrigações dos agentes envolvidos no tratamento de dados, a garantia de direitos substantivos aos titulares de dados pessoais e a instituição de autoridades nacionais de proteção de dados nos Estados-membros.[210] Essas autoridades são responsáveis por fiscalizar e aplicar as normas dentro dos limites territoriais de seu Estado-membro, bem como em situações que envolvam relações extraterritoriais ligadas ao seu território. Todo indivíduo situado na União Europeia, em princípio, pode fazer valer direitos subjetivos perante essas autoridades. Isso também é válido para a administração da UE, que é supervisionada pela Autoridade Europeia de Proteção de Dados. Paralelamente, o Comitê Europeu de Proteção de Dados desempenha um papel de coordenação entre as autoridades nacionais, tendo substituído o antigo Grupo de Trabalho Artigo 29 após o advento do RGPD.[211]

---

[207] LYNSKEY, Orla. **The foundations of EU data protection law**. Oxford University Press, 2015. p. 66.

[208] SCHWARTZ; PEIFER, 2017. p. 129.

[209] HELBERGER, Natali; BORGESIUS, Frederik Zuiderveen; REYNA, Agustin. The perfect match? A closer look at the relationship between EU consumer law and data protection law. **Common Market Law Review**, v. 54, n. 5, 2017. pp. 28.

[210] GIURGIU, Andra; LARSEN, Tine A. Roles and powers of national data protection authorities. **European Data Protection Law Review**, v. 2, n. 3, 2016. p. 342. Disponível em: https://www.semanticscholar.org/paper/Roles-and-Powers-of-National-Data-Protection-Giurgiu-Larsen/fb3e33026e4a0e86eb55c64cf4888294ed5b9ed0?p2df. Acesso em: 2 nov. 2023.

[211] VERONESE, Alexandre; SANTOS, Luiza Mendonça da Silva Belo. Padrões de conformidade nacionais de proteção de dados pessoais: anotações na perspectiva de compliance após a invalidação do privacy shield firmado entre os Estados Unidos da América e a União Europeia. In: CUÊVA, Ricardo; FRAZÃO, Ana, **Compliance e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021. pp. 100-101.

A Diretiva UE 680/2016, em conjunto com o RGPD, compõe o quadro legal para a proteção de dados na UE. [212] Essa normativa, também conhecida como *Law Enforcement Directive* (LED), possui um escopo mais restrito quando comparado ao RGPD, sendo aplicável ao tratamento de dados pessoais por autoridades competentes de cumprimento da lei, com o objetivo de prevenir, investigar, detectar ou reprimir infrações penais ou executar sanções penais, incluindo a proteção contra ameaças à segurança pública e sua prevenção. Importa destacar que as atividades voltadas à segurança e a defesa nacional não estão incluídas nesse diploma normativo. A LED foi concebida para buscar um equilíbrio entre o direito à proteção de dados e as necessidades e os objetivos da persecução penal e de segurança pública. Sendo uma diretiva, os Estados-membros devem proceder à sua transposição para os seus ordenamentos jurídicos nacionais, o que já foi realizado pela maioria deles.

Ambos, o RGPD e a LED, introduziram regimes de tutela para as transferências de dados pessoais para além das fronteiras europeias, os quais serão objeto da análise seguinte.

2.1.1.1. Os regimes de tutela para as transferências internacionais de dados pessoais no RGPD

O RGPD instituiu regimes estritos para as transferências de dados pessoais a países terceiros, que são disciplinados em três parâmetros diferentes de proteção. A premissa central do RGPD reside no requisito de adequação, que já era previsto na Diretiva 95/46/CE.[213] Este requisito autoriza transferências internacionais de dados pessoais caso o país terceiro apresente um nível de proteção adequado, conforme uma avaliação conduzida pela Comissão Europeia.

A decisão de adequação eleva o país terceiro à posição de equivalência com qualquer Estado-membro da UE no contexto de transferências internacionais de dados. Uma vez conferida a decisão, o país está habilitado a receber dados pessoais a partir da

---

[212] UNIÃO EUROPEIA. **Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho**. Bruxelas, 27 abr. 2016. Disponível em: http://data.europa.eu/eli/dir/2016/680/oj. Acesso em: 2 nov. 2023.

[213] COMISSAO EUROPEIA. **How the EU determines if a non-EU country has an adequate level of data protection**. 2023. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#adequacy-decisions-latest. Acesso em: 2 nov. 2023.

UE sem que requisitos adicionais sejam necessários. Com efeito, após uniformizar a proteção de dados entre seus Estados-membros, a UE busca evitar que dados pessoais sejam transferidos para países terceiros com baixos padrões de proteção. Como será detalhado na Seção 2.2, o requisito da adequação da UE contribuiu de maneira substancial para a adoção de leis gerais de proteção de dados ao redor do mundo, incluindo na América Latina.

No que se refere ao conteúdo das decisões de adequação, a Comissão Europeia considera um conjunto amplo de fatores estabelecidos no artigo 45 do RGPD, incluindo o respeito aos direitos humanos e liberdades fundamentais, a existência de leis de proteção de dados, a garantia de direitos para os titulares dos dados e de recursos judiciais e administrativos, a presença de autoridades supervisoras independentes, os compromissos internacionais ou outras obrigações decorrentes de instrumentos internacionais vinculantes e a participação em sistemas multilaterais ou regionais de proteção de dados pessoais.

O procedimento se inicia com diálogos e tratativas entre a Comissão Europeia e o país terceiro em questão. Tais iniciativas podem exigir que o país em análise altere suas legislações referentes à proteção de dados ou forneça garantias à UE. O curso do processo compreende uma proposta da Comissão Europeia, seguida por uma opinião do Comitê Europeu de Proteção de Dados. Posteriormente, a aprovação dos representantes dos Estados-membros da UE é solicitada, culminando na adoção da decisão final proferida pela Comissão Europeia. Cabe destacar que o Parlamento Europeu e o Conselho da UE podem ser envolvidos em qualquer fase do processo, uma vez que detêm a prerrogativa de requerer à Comissão que modifique ou revogue uma decisão de adequação. As bases constitucionais da proteção de dados na UE também possibilitam a manutenção de um papel contínuo do Tribunal de Justiça da UE (TJUE) na revisão da legalidade da decisão de adequação. [214]

Atualmente, os países que atendem aos critérios de adequação da UE compreendem uma lista enxuta. Na avaliação de Anupam Chander e Paul M. Schwartz, o processo daUE para avaliação da adequação de países terceiros demonstra certa limitação em acompanhar o aumento dos fluxos transfronteiriços de dados.[215] A

[214] COMISSAO EUROPEIA. **How the EU determines if a non-EU country has an adequate level of data protection**. 2023. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#adequacy-decisions-latest. Acesso em: 2 nov. 2023.

[215] CHANDER; SCHWARTZ, 2023. p. 74.

complexidade do processo também pode aumentar os custos de conformidade, criando obstáculos para que países em desenvolvimento sejam considerados adequados.[216] Ainda, os autores assinalam que a Comissão Europeia reconhece que a abertura de um diálogo sobre adequação é influenciada por fatores diversos, como a extensão das relações comerciais e políticas entre a UE e o país terceiro, particularmente a promoção de valores comuns e objetivos compartilhados a nível internacional, além da influência do país como um modelo para os demais países em sua região.[217-218]

Na ausência de uma decisão de adequação, as transferências internacionais de dados podem ocorrer mediante salvaguardas apropriadas e sob a condição de que os direitos do titular dos dados sejam executáveis e remédios legais eficazes estejam disponíveis, nos termos dos artigos 46 e 47 do RGPD. Essas salvaguardas podem ser baseadas em cláusulas contratuais padrão, normas corporativas vinculantes, códigos de conduta e certificações aprovadas, oferecendo soluções para que agentes envolvidos na transferência possam seguir voluntariamente os padrões da UE. Embora sirvam como alternativas ao requisito de adequação, tais mecanismos possuem critérios rigorosos, sobretudo no caso de transferências ulteriores. Com relação às cláusulas contratuais padrão, em 2021, a Comissão Europeia emitiu um conjunto de cláusulas modernizadas de acordo com o RGPD, substituindo as anteriores que haviam sido adotadas sob a Diretiva 95/46/CE.[219]

Além disso, as transferências também podem ser baseadas nas denominadas derrogações, as quais servem como exceções aos requisitos de que os dados pessoais só podem ser transferidos se o país terceiro tiver um nível de proteção adequado ou se salvaguardas apropriadas forem adotadas. São exemplos de derrogações o consentimento do titular, a execução de um contrato ou razões relevantes de interesse público, conforme o artigo 49 do RGPD. O Comitê Europeu de Proteção de Dados estabelece que as derrogações devem ser interpretadas de maneira restritiva para que a exceção não se torne

---

[216] CHANDER; SCHWARTZ, 2023. p. 94.
[217] CHANDER; SCHWARTZ, 2023. pp. 93-94.
[218] COMISSÃO EUROPEIA. Digital Single Market – **Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers**. 10 jan. 2017. Disponível em: https://ec.europa.eu/commission/presscorner/detail/de/MEMO_17_15. Acesso em: 2 nov. 2023.
[219] COMISSÃO EUROPEIA. **Standard contractual clauses for data transfers between EU and non-EU countries**. 2021. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en. Acesso em: 2 nov. 2023.

a regra, o que também é apoiado pela redação do RGPD que afirma que as derrogações devem ser usadas para situações específicas.[220]

2.1.1.2. Os regimes de tutela para as transferências internacionais de dados pessoais na LED

Sob a LED, a lógica aplicada às transferências internacionais de dados pessoais se difere do RGPD, apesar de ambos compartilharem uma estrutura similar. [221] As transferências internacionais, segundo o artigo 36 da LED, devem estar respaldadas por uma decisão de adequação da Comissão Europeia, assim como no RGPD, mas somente são permitidas por parte de autoridades competentes e para fins de prevenção, investigação, detecção ou repressão de infrações penais ou execução de penalidades criminais, incluindo a proteção contra ameaças à segurança pública e sua prevenção. O país terceiro, portanto, deve ser capaz de fornecer um nível de proteção adequado aos padrões da UE.

Na falta de uma decisão de adequação, as transferências internacionais de dados pessoais podem ser realizadas mediante salvaguardas apropriadas. O artigo 37 da LED oferece duas opções distintas. A primeira é a transferência com base em um instrumento juridicamente vinculativo. A segunda permite a transferência baseada na avaliação do controlador, que deve analisar todas as circunstâncias inerentes à transferência, conforme os padrões de proteção de dados do país receptor, informar as categorias de dados envolvidas na transferência à APD e documentar a transferência para possível revisão da autoridade.

As transferências internacionais de dados pessoais também podem ocorrer no caso das derrogações previstas no artigo 38 da LED, que estabelecem situações específicas e tem como objetivos, entre outros, proteger interesses vitais e/ou legítimos do titular dos dados, prevenir ameaças iminentes e graves contra a segurança pública de um Estado-membro ou país terceiro, e apoiar o exercício ou defesa de um direito em processo judicial. Ainda, o artigo 39 da LED institui uma estrutura para transferências de

---

[220] EUROPEAN DATA PROTECTION BOARD. **Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679**. 25 mai. 2018. pp. 17. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf Acesso em: 2 nov. 2023.

[221] SAJFERT, Juraj; QUINTEL, Teresa. **Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities**. 2017. pp.22. Disponível em: https://ssrn.com/abstract=3285873 ou http://dx.doi.org/10.2139/ssrn.3285873. Acesso em: 2 nov. 2023.

dados pessoais diretamente para destinatários estabelecidos em países terceiros sob condições particulares.

Após a análise do modelo jurídico de proteção de dados da UE, juntamente com as normativas e regimes de tutela das transferências internacionais de dados pessoais correspondentes, a Seção seguinte se concentra no modelo jurídico dos EUA. Essa transição permite examinar as distintas abordagens adotadas pelas duas regiões para a proteção de dados.

2.1.2. O modelo jurídico de proteção da privacidade da informação dos EUA

Nos EUA, a expressão mais utilizada para se referir à proteção conferida aos dados pessoais constitui "privacidade da informação" (em inglês, *information privacy*).[222] Essa terminologia será aplicada ao longo desta Seção. Apesar do destaque dos EUA nas discussões iniciais sobre a proteção da privacidade da informação, ao estabelecer linhas gerais para a criação de um código de boas práticas no relatório produzido pelo governo federal em 1973, conforme analisado na Seção 1.2.1, o modelo regulatório norte-americano sobre o tema divergiu daquela que se consolidou no espaço europeu.

A Constituição Federal dos EUA não menciona expressamente o direito à privacidade. No entanto, esse direito pode ser extraído da Primeira Emenda, que confere o direito de manter em sigilo as afiliações a grupos ou organizações, da Terceira Emenda, que protege o direito à privacidade do lar, e da Quarta Emenda, que impõe limitações contra buscas e apreensões irrazoáveis.[223] O foco primordial da evolução constitucional da privacidade da informação era aumentar a proteção dos cidadãos contra a interveniência estatal. Em determinados Estados da federação, por sua vez, há disposições constitucionais que diretamente estabelecem o direito à proteção da privacidade.[224]

Nas relações jurídicas entre particulares, a proteção da privacidade da informação no modelo dos EUA tem sido orientada sob a ótica de mercado, frequentemente dentro do contexto de defesa do consumidor. O seu objetivo é garantir que a coleta e o uso de dados pessoais sejam realizados de maneira justa e transparente e que os consumidores tenham um grau de controle sobre como seus dados são utilizados. Nesse sentido, o desenvolvimento da proteção da privacidade da informação nos EUA se

[222] CHANDER; SCHWARTZ, 2023. p. 55.
[223] SOLOVE, Daniel J.; SCHWARTZ, Paul M. **Information privacy law**. Aspen Publishing, 18 nov. 2020. p. 1346.
[224] SOLOVE; SCHWARTZ, 2020. pp. 75-76.

deu, em grande parte, pela jurisprudência na forma de reparações por violações de privacidade tanto em contextos contratuais quanto extracontratuais.[225]

Além disso, o modelo norte-americano de privacidade da informação é setorial e contempla uma combinação de leis em níveis federal e estadual, regulamentações e autorregulação.[226] Diante da sua tradição jurídica e constitucional,[227] ao longo do tempo, os EUA têm resistido à implementação de uma legislação abrangente federal para a privacidade da informação, mantendo o seu modelo fragmentado. Contudo, essa tendência aparenta estar em processo de mudança. Em outubro de 2023, o Presidente Joe Biden divulgou a Ordem Executiva sobre o Desenvolvimento, Uso Seguro, Protegido e Confiável de Inteligência Artificial (em inglês, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* – IA), que discute, em parte, a necessidade de se estabelecer uma legislação federal abrangente de privacidade da informação nos EUA.[228]

Para proteger a privacidade de todos os cidadãos norte-americanos, incluindo quanto aos riscos apresentados pela IA, a Ordem Executiva sugere a aprovação pelo Congresso de uma legislação bipartidária de privacidade da informação.[229] A compreensão de que práticas de proteção de dados sólidas se traduzem em benefícios econômicos igualmente tem impulsionado o movimento. Esse avanço legislativo pode representar uma mudança significativa na abordagem jurídica dos EUA no tema, sinalizando uma aproximação com os padrões regulatórios de proteção de dados da UE.

No atual quadro fragmentado, há leis federais relacionadas à privacidade em setores específicos. O *Fair Credit Reporting Act,* de 1970 e o *Fair and Accurate Credit Transactions Act,* de 2003, conferem direitos sobre o uso e a divulgação de dados pessoais por agências de relatórios de crédito. O *Children's Online Privacy Protection Act,* de

---

[225] VERONESE, 2021. p. 701.

[226] SCHWARTZ; PEIFER, 2017. pp. 132-133.

[227] BERMAN, Paul Schiff. Cyberspace and the state action debate: the cultural value of applying constitutional norms to private regulation. **University of Colorado Law Review**, v. 71, 4 mai. 2000. p. p. 1266. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=228466. Acesso em: 2 nov. 2023.

[228] ESTADOS UNIDOS. The White House. **Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence**. Washington, 30 jun. 2023. Disponível em: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/. Acesso em: 2 nov. 2023.

[229] ESTADOS UNIDOS. The White House. **FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence**. Washington, 30 jun. 2023. Disponível em: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/. Acesso em: 2 nov. 2023.

1998, restringe o uso de dados coletadas de crianças na Internet, entre outros. [230] Apesar de determinados setores não estarem compreendidos por leis federais voltadas à proteção da privacidade da informação, cabe notar que as empresas podem estar sujeitas à atuação da *Federal Trade Commission* (FTC), que tem poderes para regular as denominadas práticas enganosas e desleais.

A FTC foi originalmente estabelecida para promover a concorrência. Suas atribuições evoluíram com o *Wheeler-Lea Act,* de 1938, quando passou a agir contra práticas que violassem os direitos de consumidores. A privacidade da informação entrou em seu escopo somente no final dos anos 1990, impulsionada pela expansão do acesso à Internet e pelas iniciativas regulatórias para proteger a crescente coleta de dados pessoais, como a Diretiva 95/46/CE da UE. Nas décadas seguintes, a FTC ampliou seu controle nessa área, sobretudo com o estabelecimento da Divisão de Privacidade e Proteção da Identidade, em 2007.[231]

Nos âmbito dos Estados, o *California Consumer Privacy Act* (CCPA), de 2018, foi a primeira legislação abrangente de privacidade implementada por um Estado.[232] Esse texto legal protege dados pessoais de consumidores na Califórnia, exigindo que os agentes cumpram obrigações de transparência. O CCPA garante aos consumidores o direito de acessar e solicitar a eliminação de seus dados pessoais, além de recusar a venda de tais dados e de serem protegidos contra discriminação ao exercer quaisquer dos direitos garantidos pela normativa. Em 2020, foi aprovado o *California Privacy Rights Act* (CPRA), uma emenda à CCPA que amplia as proteções aos consumidores e as obrigações às empresas.[233]

Diferentemente da UE, os EUA não adotaram regimes estritos para as transferências internacionais de dados pessoais, contudo, fazem parte do sistema CBPR da APEC, além de se engajarem no Fórum Global CBPR, conforme analisado na Seção 1.2.5 anterior.[234] Cabe uma nota também a respeito de padrões de cooperação na

---

[230] SOLOVE; SCHWARTZ, 2020. pp. 77-78.

[231] FONSECA, Mariana Moutinho. **The Federal Trade Commission Against Facebook: a law and society approach to consumer privacy and competition policy**. Dissertação (Mestrado em Direito), Universidade de Brasília, Brasília, 2021. Disponível em: https://repositorio.unb.br/browse?type=author&value=Fonseca%2C+Mariana+Moutinho. Acesso em: 2 nov. 2023.

[232] ESTADOS UNIDOS. **California Consumer Privacy Act of 2018**, Cal. Civ. Code §§ 1798.100 a 1798.199. Disponível em: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 Acesso em: 2 nov. 2023.

[233] SOLOVE; SCHWARTZ. 2020. p.79.

[234] SCHWARTZ; PEIFER, 2017. pp. 95-97.

persecução penal nos EUA. O *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act) é uma legislação federal que surgiu, entre outros motivos, como resposta à dificuldade enfrentada pelas autoridades norte-americanas para acessar dados relevantes para investigações criminais armazenados em servidores em outros países. O CLOUD Act incluiu a Seção 2523 no Título 18 do *United States Code*, que trata da possibilidade de que os EUA firmem acordos executivos com países estrangeiros para que haja um fluxo de dados entre eles, com o intuito de combater atividades criminosas.[235-236]

No decorrer do tempo, a UE e os EUA têm trabalhado juntos para estabelecer programas voluntários de autocertificação para as transferências internacionais de dados pessoais, tais como o *Safe Harbor*, o *Privacy Shield* e o atual *Data Privacy Framework*. Esses esforços visam a promover a interoperabilidade entre os modelos de proteção à privacidade e aos dados pessoais de cada região. Entretanto, os debates em torno desses programas ampliaram as tensões entre a UE e os EUA, trazendo à tona desafios significativos na transferência transatlântica de dados pessoais, o que será analisado a seguir.

2.1.3. O conflito transatlântico em torno das transferências de dados pessoais entre UE-EUA: fluxos comerciais e civis

O problema da interconexão jurídica entre UE e EUA nos fluxos de dados já havia sido alertado por Joel R. Reidenberg no seu estudo sobre o ciberespaço.[237] Como resultado das diferenças entre os modelos de proteção à privacidade e aos dados pessoais da UE e dos EUA, a Comissão Europeia considerou que os EUA não forneciam um nível de proteção de dados adequado sob a égide da Diretiva 95/46/CE.[238] Diante disso, ao longo dos anos, ambos os lados têm unido esforços para desenvolver mecanismos que possam conferir interoperabilidade entre os seus padrões para facilitar as transferências

[235] ESTADOS UNIDOS. **H.R.4943 – CLOUD Act – 115th Congress (2017-2018)**. Washington, 2 jun. 2018. Disponível em: https://www.congress.gov/bill/115th-congress/house-bill/4943/text; Acesso em: 2 nov. 2023.

[236] CORNELL LAW SCHOOL. Legal Information Project. **18 U.S. Code § 2523 - Executive agreements on access to data by foreign governments**. Ithaca, 2021. Disponível em: https://www.law.cornell.edu/uscode/text/18/2523. Acesso em: 2 nov. 2023.

[237] REIDENBERG, 1996. p. 913.

[238] UNIÃO EUROPEIA. Working Party. **Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government (5092/98/EN/final/WP15)**, 26 jan. 1999. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp15_en.pdf. Acesso em: 2 nov. 2023.

transatlânticas de dados pessoais no âmbito comercial e civil.[239] Representados pela Comissão Europeia e pelo Departamento de Comércio, respectivamente, a UE e os EUA negociaram os fundamentos de programas voluntários de autocertificação em 2000, com o *Safe Harbor*,[240] e em 2016, com o *Privacy Shield,*[241] que foram materializados por meio de decisões de adequação da Comissão Europeia.

Segundo Paul Schiff Berman, os arranjos propostos representavam uma combinação dos padrões de proteção de dados adotados por cada região.[242] O modelo dos programas de autocertificação do *Safe Harbor* e do *Privacy Shield* se baseava no compromisso por parte das empresas norte-americanas de aderir a um conjunto de padrões de proteção para transferir dados pessoais a partir da UE. Para tanto, as empresas deveriam autocertificar a sua conformidade com tais padrões e atestar essa avaliação em um registro público *online*. Isso estabeleceu uma via que permitiu às empresas norte-americanas expandir a oferta de bens e serviços para o mercado europeu, sobretudo no setor de tecnologia.[243] A adesão aos padrões era supervisionada por órgãos federais americanos, incluindo a FTC.[244]

No entanto, em cada caso, o TJUE destacou inconsistências críticas nos mecanismos e os invalidou. O conflito resultante entre a UE e os EUA foi denominado por diversos autores como "guerra transatlântica de dados".[245-246] Esse conflito foi, incialmente, impulsionado pelas revelações de Edward Snowden sobre os programas da Agência de Segurança Nacional dos EUA, que impactaram negativamente a confiança nas transferências internacionais de dados pessoais entre a UE e os EUA sob o *Safe Harbor.* Em 2013, o austríaco Maximillian Schrems recorreu à autoridade irlandesa de

---

[239] HEISENBERG, Dorothee. **Negotiating Privacy: The European Union, the United States, and Personal Protection**. Lynne Rienner Publishers, 2005.

[240] UNIÃO EUROPEIA: Comissão das Comunidades Europeias. **2000/520/CE: Decisão da Comissão, de 26 de Julho de 2000, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de proteção assegurado pelos princípios de "porto seguro" e pelas respectivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América.** Bruxelas, 26 ago. 2000. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32000D0520. Acesso em: 2 nov. 2023.

[241] COMISSÃO EUROPEIA: **Commission implementing decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield C (2016) 4176 final**. Bruxelas, 12 jul. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG. Acesso em: 2 nov. 2023.

[242] BERMAN, 2006. p. 1128.

[243] FARRELL, Henry; NEWMAN, Abraham L. **Of privacy and power: The transatlantic struggle over freedom and security**. Princeton University Press, 2 abr. 2019. pp. 248.

[244] CHANDER; SCHWARTZ, 2023. p. 100.

[245] SCHWARTZ; PEIFER, 2017. p. 117.

[246] FARRELL, Henry; NEWMAN, Abraham. The transatlantic data war: Europe fights back against the NSA. **Foreign Affairs**, v. 95, n. 1, pp.124-133, jan/fev. 2016. p. 157.

proteção de dados para contestar a transferência de dados pessoais a partir da empresa Facebook Ireland Ltd para empresa do mesmo grupo, situada os EUA.

O caso Schrems I chegou ao TJUE, que, em 2015, invalidou o *Safe Harbor* devido a dois principais problemas identificados.[247] O primeiro, era que o arranjo não restringia adequadamente o acesso pelo governo e programas de segurança norte-americanos aos dados pessoais transferidos da UE por agentes privados em circunstâncias comerciais. O segundo, residia no fato de que o TJUE estava preocupado com a aprovação única, e não contínua, da adequação do *Safe Harbor* pela Comissão Europeia. O TJUE declarou que seria responsabilidade da Comissão revisar periodicamente se a adequação do nível de proteção garantido pelo país terceiro continuaria sendo válida, tanto factual quanto juridicamente. Ainda, o TJUE concluiu que o nível de proteção de um país terceiro deveria ser essencialmente equivalente ao nível fornecido pelos Estados-membros da UE.

Os problemas indicados pelo TJUE foram endereçados pelo *Privacy Shield*, que veio a substituir o *Safe Harbor*. O diretor de Inteligência Nacional dos EUA apresentou garantias específicas relativas à proteção dos dados. Também foi instaurado um órgão no Departamento de Estado dos EUA para tratar de reclamações individuais da UE relacionadas ao acesso à dados pessoais no contexto de segurança (em inglês, *Privacy Shield Ombudsperson*) e implementado um processo que permitiu à Comissão revisar a sua decisão adequação. Ainda que o *Privacy Shield* tenha sido submetido a duas revisões anuais conjuntas entre a UE e os EUA, o mecanismo foi invalidado no caso Schrems II pelo TJUE em 2020, sob o fundamento de que o arranjo não oferecia um nível de proteção essencialmente equivalente ao da UE, novamente diante do acesso a dados pessoais transferidos por agentes privados no âmbito dos programas de segurança norte-americanos.[248] O TJUE apontou a falta de limitações no acesso em larga escala a dados pessoais, a ausência de remédios legais eficazes disponíveis para os titulares de dados da UE e a insuficiência do órgão do Departamento de Estado para receber reclamações.

Em que pese a invalidação do *Privacy Shield*, o TJUE considerou que as transferências internacionais de dados pessoais com base nas cláusulas contratuais padrão

---

[247] UNIÃO EUROPEIA: Tribunal de Justiça. **Acórdão (Grande Seção) de 6 out. 2015: Maximillian Schrems contra Data Protection Commissioner (processo C-362/14)**. Luxemburgo, 6 out. 2015. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62014CJ0362. Acesso em: 2 nov. 2023.

[248] UNIÃO EUROPEIA: Tribunal de Justiça. **Acórdão do Tribunal de Justiça (Grande Secção) de 16 de julho de 2020 - Data Protection Commissioner contra Facebook Ireland Ltd e Maximillian Schrems (Processo C-311/18)**. Luxemburgo, 16 jul. 2020. Disponível em: http://curia.europa.eu/juris/liste.jsf?num=C-311/18. Acesso em: 2 nov. 2023.

aprovadas pela Comissão Europeia permaneciam válidas, contanto que os agentes envolvidos na transferência pudessem conduzir uma avaliação de risco sobre o nível de proteção do país terceiro, incluindo a análise de leis que estabeleçam a possibilidade de divulgar dados pessoais às autoridades públicas no país em questão, e que medidas suplementares fossem adotadas para assegurar a efetividade do cumprimento dos padrões europeus, quando necessário. Segundo as recomendações posteriormente emitidas pelo Comitê Europeu de Proteção de Dados, tais medidas podem ter caráter contratual, organizacional ou técnico, de modo a suprir quaisquer inadequações nas leis do país terceiro em relação aos padrões europeus.[249]

Cabe ressaltar que, em ambas as decisões de Schrems, o TJUE fortaleceu o papel das autoridades nacionais de proteção de dados nos Estados-membros da UE. O TJUE determinou que cada autoridade está investida do poder de examinar se uma transferência de dados pessoais de seu próprio Estado-Membro para um país terceiro cumpre os requisitos estabelecidos no RGPD.[250] Mais recentemente, isso foi observado na investigação conduzida pela APD da Irlanda (em inglês, *Irish Data Protection Commission,* IDPC), que resultou na decisão de maio de 2023 que estabeleceu que as cláusulas contratuais padrão e as medidas suplementares empregadas pela empresa Meta Platforms Ireland Ltd não eram suficientes para garantir a segurança das transferências de dados pessoais a partir da UE para os EUA, já que não endereçavam adequadamente os riscos para os direitos e liberdades dos cidadãos da UE.[251]

O IDPC identificou que as cláusulas contratuais padrão seriam ineficazes neste caso, uma vez que as leis dos EUA, em particular, o *Foreign Intelligence Surveillance Act* (FISA), poderiam contradizer os termos das cláusulas e que as medidas suplementares apresentadas pela empresa não seriam capazes de suprir tais inadequações, comprometendo a proteção contratualmente assegurada aos titulares dos dados. Também

---

[249] EUROPEAN DATA PROTECTION BOARD. **Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.** 18 jun. 2021. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en. Acesso em: 2 nov. 2023.

[250] WEISS, Martin A.; ARCHICK, Kristin. **US-EU data privacy: from safe harbor to privacy shield**. Washington, DC: Congressional Research System, 19 mai. 2016. p. 7. Disponível em: https://www2.epic.org/crs/R44257.pdf. Acesso em: 2 nov. 2023.

[251] DATA PROTECTION COMMISSION. **Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation**. Dublin, 22 maio 2023. Disponível em: https://edpb.europa.eu/our-work-tools/consistency-findings/register-decisions/2023/decision-data-protection-commission_en. Acesso em: 2 nov. 2023.

foi constatado pelo IDPC que as transferências não poderiam ser justificados por nenhuma das derrogações previstas no RGPD. As conclusões do IDPC foram submetidas à análise de outras APD europeias e o caso foi encaminhado ao Comitê Europeu de Proteção de Dados para uma resolução definitiva.

Com as contribuições do Comitê, o IDPC impôs uma penalidade de € 1,2 bilhão, exigiu a suspensão de todas as transferências de dados pessoais da UE para os EUA no prazo de cinco meses e determinou que a empresa alinhasse as suas práticas de tratamento de dados com o RGPD. Embora a decisão seja vinculante apenas para a empresa Meta, o IDPC sugere que o mesmo racional pode ser aplicado em investigações relacionadas a outras empresas que estão sob o escopo do FISA e que fazem uso de cláusulas contratuais padrão para transferir dados pessoais da UE para os EUA.

O acirramento do conflito transatlântico pelas decisões do TJUE e do IDPC sublinhou um problema reiterado no que se refere à transferência de dados pessoais entre as regiões. Nas decisões, foi evidenciado que os EUA têm buscado acessar dados pessoais por razões de segurança, mas dependem fortemente do setor privado para obter tais dados. Nessa dinâmica de monitoramento pulverizada,[252] o mesmo ocorre em nível nacional e internacional. Assim, o atendimento às requisições de acesso a dados pessoais por parte de autoridades públicas de um país pode expor entidades privadas ao descumprimento das leis de proteção de dados do local onde esses dados foram originalmente coletados.[253] Há uma sobreposição, portanto, entre os mecanismos que regulam as transferências internacionais de dados pessoais e as normas que se aplicam à segurança.[254]

Isso ressalta a necessidade de que sejam estabelecidas balizas para a proteção integral de dados, abrangendo contextos diversos que envolvem atividades de segurança e a investigação e repressão criminal. Em alguns casos, as agências de inteligência e as autoridades voltadas à persecução penal fazem parte da mesma estrutura organizacional e os dados podem ser compartilhados entre elas. Com efeito, deve haver um esforço para compreender como os setores público e privado atualmente se relacionam nas atividades de segurança.[255] Nesse sentido, o conflito travado entre UE e EUA não apenas evidencia

[252] ZUBOFF, Shoshana. The age of surveillance capitalism: The fight for a human future at the new frontier of power. New York: PublicAffairs, 2019. p. 82.
[253] FARRELL; NEWMAN; 2019. pp. 157-158.
[254] CATE, Fred H.; DEMPSEY, James X.; RUBINSTEIN, Ira S. Systematic government access to private-sector data. **International Data Privacy Law**, v. 2, n. 4, p. p. 2012. pp. 195-199.
[255] FARRELL; NEWMAN; 2019. pp. 166-167.

as suas diferentes tradições jurídicas, mas enseja uma reflexão sobre a proteção integral dos dados pessoais.

Cabe notar que o acesso a dados por autoridades públicas estrangeiras também motivou discussões em torno da imposição de requisitos para a localização de dados pessoais (em inglês, *data localization*), como é o caso de obrigações que determinam o armazenamento de dados em repositórios situados em territórios nacionais.[256] A despeito disso, requisitos rígidos de localização podem não ser adequados para evitar o acesso a dados pessoais por autoridades públicas estrangeiras em um cenário econômico, político e social que, cada vez mais, exige os fluxos de dados entre países.

Assim, conforme analisado nesta Seção, a tensão entre a UE e os EUA tem desafiado a consolidação de um quadro estável para as transferências de dados pessoais entre as duas regiões. Esse cenário envolve a preservação da proteção e dos direitos dos titulares cujos dados são transferidos, atividades de segurança e a viabilidade econômica de indústrias que dependem das transferências internacionais de dados pessoais para seus negócios. Diante desse panorama, uma nova tentativa de solução foi proposta por meio do *Data Privacy Framework*, que será examinado a seguir.

2.1.3.1. O *Data Privacy Framework* UE-EUA

O conflito entre a UE e os EUA encontrou um novo caminho para a resolução, por meio de um substituto para o *Privacy Shield*, denominado de *Data Privacy Framework*. Em julho de 2023, esse mecanismo entrou em vigor a partir da adoção de uma decisão de adequação da Comissão Europeia. [257] As empresas norte-americanas podem aderir ao *Data Privacy Framework* comprometendo-se a cumprir um conjunto de obrigações de proteção de dados, como, por exemplo, a exigência de excluir dados pessoais que não são mais necessários para a finalidade para qual foram coletados e a garantia de continuidade da proteção quando os dados forem compartilhados com terceiros.

---

[256] CENTRE FOR INFORMATION POLICY LEADERSHIP. **Data Localization and Government Access to Data Stored Abroad,** mar. 2023. pp. 8. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-tls_discussion_paper_ii_data_localization_and_government_access_to_data_stored_abroad__29_march_2023__2_.pdf. Acesso em: 2 nov. 2023.

[257] COMISSÃO EUROPEIA. **Commission implementing decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework**. Bruxelas, 10 jul. 2023. p. 136. Disponível em: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf . Acesso em: 2 nov. 2023.

O funcionamento do *Data Privacy Framework* será objeto de revisões periódicas, conduzidas pela Comissão Europeia em conjunto com representantes das APD europeias e de autoridades relevantes dos EUA. A administração do mecanismo fica a cargo do Departamento de Comércio dos EUA, responsável por analisar os pedidos de certificação e por verificar se as empresas participantes mantêm a conformidade com os critérios de certificação. O cumprimento das obrigações assumidas pelas empresas norte-americanas conforme o *Data Privacy Framework* será supervisionado pela FTC.[258]

Um elemento distintivo que serviu de base para a decisão de adequação da Comissão diz respeito à Ordem Executiva dos EUA para o Fortalecimento das Proteções das Atividades de Inteligência de Sinais (em inglês, *Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities*).[259] Essa Ordem Executiva, assinada pelo Presidente Biden, em outubro de 2022, busca endereçar os problemas apontados pelo TJUE no caso Schrems II. Nesse sentido, a Ordem Executiva prevê garantias que limitam o acesso a dados pessoais pelas autoridades públicas norte-americanas ao que é necessário e proporcional nas atividades de segurança.

Da mesma forma, a Ordem Executiva estabelece mecanismos em camadas para tratar e resolver reclamações a respeito do uso de dados pessoais para fins de segurança. Isso inclui o estabelecimento de um Oficial de Proteção às Liberdades Civis (em inglês, *Civil Liberties Protection Officer*) e de uma Corte de Revisão de Proteção de Dados (em inglês, *Data Protection Review Court*). Na UE, as reclamações podem ser apresentadas pelos titulares às APD dos Estados-membros e serão transmitidas aos EUA pelo Comitê Europeu de Proteção de Dados. [260]

Apesar de servir como resposta às preocupações europeias sobre as atividades de segurança norte-americanas, a Ordem Executiva amplia as suas salvaguardas para além da relação UE-EUA. A Ordem Executiva estabelece que deve ser considerado o respeito à privacidade e liberdades civis de todos os indivíduos no âmbito das atividades de segurança, independentemente da nacionalidade ou local de residência. Ainda, os mecanismos para tratar e resolver reclamações descritos acima estão disponíveis para

[258]COMISSÃO EUROPEIA. **Questions & Answers: EU-US Data Privacy Framework**. 10 jul. 2023. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752. Acesso em: 2 nov. 2023.

[259] ESTADOS UNIDOS. The White House. **Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities (14086)**. Washington, 7 out. 2022. pp. 15. Disponível em: https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22531.pdf. Acesso em: 2 nov. 2023.

[260]COMISSÃO EUROPEIA. **Questions & Answers: EU-US Data Privacy Framework**. 10 jul. 2023. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752. Acesso em: 2 nov. 2023.

indivíduos em "Estados qualificados", que são definidos como aqueles que possuem leis que exigem garantias apropriadas na condução de atividades de inteligência de sinais para os dados pessoais de cidadãos dos EUA. A Ordem Executiva, portanto, introduz um aspecto de reciprocidade. O Procurador-Geral dos EUA tem poderes para designar os países ou integrações econômicas regionais como "Estados qualificados".[261] Atualmente, a UE já foi designada como tal.[262]

A despeito dos desafios que ameaçam a validade do *Data Privacy Framework* à luz da jurisprudência do TJUE que se consolidou em torno dos seus antecessores, é razoável concluir que a UE vem tendo impacto no estabelecimento de padrões de proteção de dados nos EUA. A Ordem Executiva tratada nesta Seção e a sinalização do Presidente Biden para que o Congresso norte-americano avance em uma legislação federal abrangente e bipartidária para a privacidade da informação nos EUA, conforme a Seção 2.1.2, demonstram que a UE tem influenciado a reformulação do modelo de proteção de dados norte-americano para que se assemelhe mais à sua própria abordagem e também incentivando outros países a seguirem esse caminho. Sob esse prisma, a Seção seguinte pretende analisar a evolução da proteção de dados no espaço latino-americano.

2.2. A evolução da proteção de dados na América Latina

A evolução da proteção de dados pessoais na América Latina possui particularidades atreladas a questões históricas, econômicas, políticas e sociais, que envolvem experiências locais, regionais e internacionais.[263] Nesta Seção, serão abordados os principais desenvolvimentos e tendências que moldaram o cenário regional de proteção de dados, incluindo as repercussões dos modelos regulatórios da UE e EUA. Cabe observar que a referência específica aos modelos de proteção de dados do Brasil, da Argentina, do Uruguai e da Colômbia será aprofundada na Seção seguinte.

Dentre os conceitos jurídicos que marcaram a construção da proteção de dados pessoais no espaço latino-americano, o *Habeas Data* se destaca como instrumento distintivo de proteção da informação e, depois, dos dados pessoais. No entanto, embora seja reconhecido como fenômeno típico do desenvolvimento da disciplina de proteção de

[261] CHANDER; SCHWARTZ, 2023. pp. 101-103.
[262] ESTADOS UNIDOS. Department of Justice. **Attorney General designations of "qualifying states" under section 3(f) of EO 14086.** Washington, 2023. Disponível em: https://www.justice.gov/opcl/executive-order-14086. Acesso em: 2 nov. 2023.
[263] PALAZZI, Pablo A. La transmisión internacional de datos personales y la protección de la privacidade: **Argentina, América Latina, Estados Unidos y Unión Europea**. Buenos Aires: Ad-hoc, 2002. p.42.

dados pessoais na América Latina, *o Habeas Data* apresenta características diversas em cada um dos países que o receberam, incluindo a sua abrangência e o seu grau de eficácia.[264] O *Habeas Data* foi idealizado a partir do constituinte brasileiro, de 1988, e espraiou-se pela América Latina, entre outras razões, como parte das medidas de ruptura com o período de ditatura militar vivenciado em determinados países da região, de modo a viabilizar o direito dos indivíduos de dispor dos seus próprios dados pessoais.[265] Nesse contexto, também é possível identificar influências externas na construção do *Habeas Data*, tais como a Constituição da Espanha, de 1978, e de Portugal, de 1976, que estabeleciam disposições sobre a utilização da informática e acesso a arquivos e registros.[266]

Em paralelo com o *Habeas Corpus*, cujo objeto constitui a tutela da liberdade pessoal, o *Habeas Data* representa um instrumento de tutela da liberdade informática.[267] De acordo com Franciso Zuñiga Urbina, a liberdade informática tem como objetivo garantir as faculdades de conhecimento e controle dos indivíduos em relação às informações que lhes dizem respeito, pretensão similar ao direito à autodeterminação informativa estabelecido na Alemanha.[268] Diante do desenvolvimento tecnológico, a liberdade informática é categorizada como uma resposta contemporânea à necessidade de proteger a crescente coleta de dados pessoais contra o possíveis prejuízos aos indivíduos.[269]

Na América Latina, destaca-se a tendência de estabelecer o *Habeas Data* como instrumento processual incorporado às Constituições nacionais de diversos países, que pode estar correlacionado a uma legislação específica.[270] Como aponta Marcela Basterra, na Argentina, na Colômbia e no Brasil, o *Habeas Data* encontra previsão nas Constituições e é acompanhado de regulamentação.[271] No Uruguai, o *Habeas Data* é reconhecido implicitamente na Constituição, porém é regulamentado na forma de lei.[272]

---

[264] DONEDA, Danilo. Iguais mas separados: o Habeas data no ordenamento brasileiro e a proteção de dados pessoais. **Cadernos da escola de direito**, n. 9, 4 abr. 2008. pp. 24-25 Disponível em: https://portaldeperiodicos.unibrasil.com.br/index.php/cadernosdireito/article/view/2607/2180. Acesso em: 2 nov. 2023.

[265] DONEDA, 2008. p. 25.

[266] DONEDA, 2008. pp. 18-19.

[267] DONEDA, 2008. pp. 20-21

[268] URBINA, Francisco Zúñiga. Derecho a la intimidad y Hábeas Data (del recurso de protección al Hábeas Data). **Derecho PUCP, v. 51,** 1997. p. 210.

[269] URBINA, 1997. p. 209

[270] URBINA, 1997. p. 210.

[271] BASTERRA, Marcela. **Protección de datos personales: la garantia de habeas data**. Buenos Aires: Ediar, 2008.

[272] BASTERRA, 2008. p. 30.

Em que pese a sua previsão normativa, em geral, o *Habeas Data* se configura como uma ação que permite efetivar direitos referentes a dados pessoais registrados em bases e bancos de dados.[273]

Os países latino-americano possuem maiores ou menores garantias jurídicas para o *Habeas Data*. Na avaliação de Oscar Raúl Puccinelli, essa variedade permite a classificação do *Habeas Data* no âmbito da região em espécies e subespécies, tipos e subtipos distintos.[274] À luz da classificação propostas por Puccinelli, na América Latina, é possível distinguir o *Habeas Data* em duas principais espécies com relação à sua finalidade. O *Habeas Data próprio* se aplica aos dados pessoais registrados em bases e bancos de dado e visa a prevenir ou reparar danos que possam ocorrer no seu tratamento. O *Habeas Data impróprio,* por sua vez, busca obter informações públicas que foram indevidamente negadas ao autor.[275] Esta última particularidade remete à motivação histórica de que o tema da proteção de dados pessoais em alguns países da América Latina se insere no contexto de reconhecimento do direto de acesso à informação e dos meios para exercer esse direito.[276]

Mais especificamente sobre o *Habeas Data próprio,* Puccinelli descreve que tal ação pode ser objeto de classificações secundárias, considerando as finalidades de cada uma delas. Por exemplo, o *Habeas Data informativo* tem como objetivo obter informações necessárias para que o autor tenha condições de avaliar se os dados pessoais estão sendo devidamente utilizados, sobretudo quando os dados não tenham sido obtidos extrajudicialmente.[277] O *Habeas Data retificador* tem como finalidade retificar ou corrigir dados pessoais imprecisos, inexatos ou incorretos que constam em bases ou bancos de dados.[278] O *Habeas Data anulador* tem o propósito de eliminar total ou parcialmente dados pessoais armazenados em bases ou bancos de dados diante de situações que não justificam a sua manutenção, como quando os dados pessoais estão sendo tratados de forma inadequada.[279]

---

[273] URBINA, 1997. p. 214.
[274] PUCCINELLI, Oscar Raúl. Evolución histórica y análisis de las diversas especies, subespecies, tipos y subtipos de habeas data en América Latina. Un intento clasificador con fines didácticos. **Vniversitas**, **n. 107**, 15 abr. 2004. pp. 471-501.
[275] PUCCINELLI, 2004. p. 488.
[276] GUADAGNA, Bruno Gaiero; BRACESCO, Ignacio M. Soba. El proceso de hábeas data en el Uruguay (protección de datos personales y acceso a la información pública). **Anuario de Derecho Constitucional Latinoamericano**. Montevideo, 2010. pp. 326-349. Disponível em: https://www.corteidh.or.cr/tablas/r28363.pdf. Acesso em: 2 nov. 2023.
[277] PUCCINELLI, 2004. p. 490.
[278] PUCCINELLI, 2004. p. 492.
[279] PUCCINELLI, 2004. p. 493.

Com relação ao momento em que a ação é iniciada e ao tipo de tutela pretendida, Puccinelli refere-se ao *Habeas Data preventivo*, cujo objetivo é evitar a consumação de danos que ainda não ocorreram, e ao *Habeas Data reparador*, aplicável em caso de danos em andamento para evitá-los ou quando esses danos já ocorreram e busca-se uma compensação financeira.[280] Ainda, o *Habeas Data* pode ser classificado segundo o alcance da legitimidade do autor da ação e os efeitos da decisão a ser proferida no processo. O *Habeas Data individual* é exercido apenas pelos indivíduos registrados em bases ou bancos de dados em relação aos seus próprios dados e a decisão tem alcance entra as partes envolvidas. Já o *Habeas Data coletivo* pode ser exercido por uma pessoa física ou pelo representante de um grupo de indivíduos cujos dados estão registrados em bases ou bancos de dados e os efeitos da decisão podem repercutir em relação a todos os afetados.[281]

Em alguns países latino-americanos, como a Argentina e a Colômbia, o *Habeas Data* permitiu o desenvolvimento de rica jurisprudência que delimitou um conjunto de princípios e direitos aos quais todo tratamento de dados pessoais deve estar sujeito.[282-283] Com efeito, ao se apoiar no *Habeas Data* como instrumento para a proteção de dados pessoais, a evolução do modelo regulatório em determinados países da região aproximou-se, inicialmente, da experiência dos EUA, na qual a proteção deve ser objeto de interpretação judicial.[284] Soma-se isso a existência de leis setoriais que regulamentam a proteção de dados em indústrias específicas.

A despeito desse cenário inicial, a construção da proteção de dados pessoais no espaço latino-americano progressivamente incorporou elementos associados à proposta regulatória da UE. Diversos países da região passaram a consolidar o entendimento segundo o qual a proteção de dados pessoais é um direito fundamental.[285] Muito embora o *Habeas Data* continue presente na maioria dos ordenamentos jurídicos dos países latino-americanos, também é notável a aprovação, ao longo das duas últimas décadas, de leis gerais de proteção de dados pessoais na América Latina, acompanhadas da criação da figura administrativa de APD, cuja inspiração reside no modelo de proteção

[280] PUCCINELLI, 2004. p. 488.
[281] PUCCINELLI, 2004. p. 489.
[282] PUCCINELLI, 2004. p. 480.
[283] SALINAS, Maria de Lourdes Zamudio. El marco normativo latinoamericano y la ley de protección de datos personales del Perú. **Revista Internacional de Protección de Datos Personales**, n. 1, jul./dez. 2012. p. 1-21. Disponível em: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok3_Ma.-de-Lourdes-Zamudio_FINAL.pdf. Acesso em: 2 nov. 2023.
[284] URBINA, 1997. p. 212.
[285] SALINAS, 2012. p. 7.

de dados da UE.[286] Na avaliação de Graham Greenleaf, o modelo europeu está se consolidando como padrão na maioria das regiões globais que possuem legislação voltadas à proteção de dados.[287]

O movimento de expansão dos padrões de proteção de dados da UE para outros países é analisado por Christopher Kuner.[288] Segundo o autor, a influência do direito europeu se deve, em parte, ao potencial benefício econômico decorrente da aprovação de leis de proteção de dados em conformidade com os padrões europeus, que impulsionariam o diálogo para receber dados pessoais transferidos a partir da UE com o respaldo de uma decisão de adequação emitida pela Comissão Europeia.[289] Esse é o caso da Argentina e do Uruguai, que foram reconhecidos como países com nível adequado de proteção. Diante dos avanços da globalização econômica e do poder do mercado europeu, o desenvolvimento do comércio internacional e eletrônico passou a exigir uma razoável compatibilidade dos parâmetros de proteção de dados pessoais para permitir os fluxos de dados entre os países envolvidos.[290] Outro aspecto consiste no escopo extraterritorial previsto no RGPD, que pode alcançar diretamente entidades em países terceiros.[291]

Além disso, o fato de o direito europeu ter se concretizado na forma de instrumentos legais claramente estruturados, tais como diretivas e regulamentos, também se tornou um atrativo para países terceiros, que optaram por se basear em textos legais existentes ao invés de elaborar uma legislação inteiramente nova.[292] Em linha com esse aspecto, Paul M. Schwartz assinala que, ao instituir um modelo abrangente de proteção de dados pessoais para possibilitar a uniformidade dos seus Estados-membros, a UE oferece uma abordagem acessível para que outros países também possam se adaptar, especialmente quando comparado ao modelo complexo e setorial dos EUA.[293]

Ainda, a difusão do modelo de proteção de dados europeu na América Latina foi corroborada pela influência da Espanha na região, tendo em vista seu legado histórico decorrente do período colonial e a proximidade linguística.[294] As leis espanholas de proteção de dados, incluindo a *Ley Orgánica de Regulación del Tratamiento*

---

[286] REIGADA, 2012. pp. 30-32.
[287] GREENLEAF, Graham. **Asian data privacy laws: trade & human rights perspectives**. OUP Oxford, 16 dez. 2014. p. 624.
[288] KUNER, 2017. pp. 128-131.
[289] KUNER, 2017. p. 132.
[290] PALAZZI, 2002. p. 39.
[291] KUNER, 2017. p. 130.
[292] KUNER, 2017. p. 131.
[293] SCHWARTZ, Paul M. Global data privacy: The EU way. **NYUL Review**, v. 94, p. 771, 22 out. 2019. pp. 810-812.
[294] PALAZZI, 2002. p. 55.

*Automatizado de los Datos de Carácter Person*al (LORTAD) de 1992,[295] e sua revisão em 1999 com a *Ley Orgánica de Protección de Datos* (LOPD), [296] inspiraram os marcos jurídicos de diversos países latino-americanos.[297] A nível regional, a criação da RIPD, em meados de 2003, também auxiliou na interlocução com a APD da Espanha.

No cenário internacional, a adesão à Convenção 108 do Conselho da Europa pelos países da América Latina foi igualmente relevante para a disseminação do tema de proteção de dados pessoais na região. Devido à facilidade de uso, rapidez e descentralização da tecnologia, o direito à proteção de dados se transformou em uma questão internacional, que passou a encontrar espaço nas agendas de diversos países.[298] A Convenção 108 representou um marco por ser o primeiro instrumento internacional vinculante destinado à proteção de dados e à transferência internacional desses dados, sob a ótica de que o direito à proteção dados é um direito fundamental. Em um mundo cada vez mais interdependente, crescia a pressão para uma política de convergência que incentivava o estabelecimento de princípios, direitos e obrigações básicas para o tratamento de dados pessoais.[299] O Uruguai foi o primeiro país da região a subscrever à Convenção, seguido pela Argentina. Outro tratado do Conselho da Europa que se expandiu na América Latina é a Convenção de Budapeste. Mais recentemente, diversos países latino-americanos aderiram a esse convênio, como o Brasil, a Argentina e a Colômbia.[300]

Além dos efeitos internacionais, a evolução da proteção de dados pessoais na América Latina também contou com a relação entre os próprios países da região, que, ao observarem seus vizinhos aderindo à implementação de sistemas de proteção de dados pessoais, passaram a ter estímulos para seguir caminho semelhante. A influência regional continua a ser percebida nos movimentos de modernização e atualização das leis de proteção de dados existentes na América Latina. Na Seção seguinte, veremos que a Argentina, pioneira na proteção de dados na América Latina, exerceu influência no

---

[295] ESPANHA. **Ley Orgánica 5/1992 de regulación del tratamiento automatizado de los datos de carácter personal.** BOE núm. 262, de 31 de octubre de 1992. 29 out. 1992. pp. 37037 a 37045. Disponível em: https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189. Acesso em: 2 nov. 2023.

[296] ESPANHA. **Ley Orgánica 15/1999 de protección de datos de carácter personal**. BOE núm. 298, de 14/12/1999. 13 dez. 1999. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750. Acesso em: 2 nov. 2023.

[297] BASTERRA, Marcela I. **Protección de datos Personales: Ley 25.326 y Dto. 1558/01 comentados - derecho constitucional provincial Iberoamérica y México**. Buenos Aires: Ediar, 2008(b). p. 23.

[298] PALAZZI, 2002. p. 46.

[299] PALAZZI, 2002, pp. 43-44.

[300] SALT, Marcos. **Nuevos desafios de la evidencia digital: acceso transfronterizo y técnicas de acesso remoto a datos informáticos**. Buenos Aires: AdHoc, 2017. pp. 255-261.

Uruguai. Mais tarde, as experiências da Argentina e do Uruguai também impactaram a Colômbia. Ainda, as discussões do Mercosul impulsionaram o marco legal do Brasil, que agora é referência em debates nos órgãos legislativos argentinos.

2.3. Breve referência aos modelos jurídicos de proteção de dados do Brasil, da Argentina, do Uruguai e da Colômbia

A trajetória da proteção de dados na América Latina reflete um esforço dos países da região para alcançar determinados objetivos, os quais incluem assegurar parâmetros mínimos de proteção aos dados pessoais,[301] garantir direitos aos titulares a que os dados se referem[302] e provê-los com recursos legais para o exercício de seus direitos, além de estabelecer deveres aos agentes responsáveis por realizar o tratamento de dados e implementar sanções e procedimentos em caso de não conformidade com as regras.[303] Esta Seção se propõe a analisar os aspectos regulatórios que compõem os modelos jurídicos de proteção de dados dos países tratados nesta pesquisa, quais sejam, Brasil, Argentina, Uruguai e Colômbia.

Para tanto, serão consideradas as disposições previstas nas constituições nacionais, as leis gerais destinadas à proteção de dados e as APD designadas para supervisionar a aplicação das leis. Além disso, também será abordada a adesão pelos países a instrumentos internacionais e regionais que circundam a temática das transferências de dados pessoais por sobre fronteiras. Ainda, serão examinadas as

---

[301] Respectivamente, as definições de dados pessoais nas leis de proteção de dados da Argentina, Uruguai, Colômbia e Brasil:
Lei nº 25.326/2000. Art. 2º: *Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.*
Lei nº 18.331/2008. Art. 4, "d": *Dato personal: información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables.*
Lei nº 1.581/2012. Art. 3º, "c": *Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.*
LGPD. Art. 5º, I: Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

[302] Respectivamente, as definições de titular dos dados nas leis de proteção de dados da Argentina, Uruguai, Colômbia e Brasil:
Lei nº 25.326/2000. Art. 2º: *Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.*
Lei nº 18.331/2008. Art. 4, "l": *Titular de los datos: persona cuyos datos sean objeto de um tratamiento incluido dentro del ámbito de acción de la presente ley.*
Lei nº 1.581/2012. Art. 3º, "f": *Titular: Persona natural cuyos datos personales sean objeto de Tratamiento.*
LGPD. Art. 5º, V: Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

[303] REMOLINA, 2015. p. 278.

decisões de adequação emitidas pela Comissão Europeia com relação ao nível de proteção de dados da Argentina e do Uruguai.

Cabe notar que a análise a seguir não pretende detalhar a totalidade de conceitos jurídicos existentes no arcabouço de proteção de dados dos países latino-americanos em questão. Em vez disso, o intuito principal é fornecer uma referência para o estudo dos regimes de tutela das transferências internacionais de dados, que constitui o cerne desta pesquisa. A divisão dos países nas Subseções seguintes está estruturada segundo a ordem cronológica de promulgação das leis gerais de proteção de dados.

2.3.1. Argentina

A partir dos anos 1980, as províncias argentinas iniciaram um processo de revisão de suas constituições, incluindo dispositivos voltados à proteção da privacidade e do *Habeas Data*.[304] A província de Buenos Aires foi pioneira ao instituir o instrumento de *Habeas Data* com expressa denominação na sua Constituição.[305] Em que pese o movimento no âmbito das províncias, com a reforma constitucional de 1994, o *Habeas Data* foi efetivamente incorporado à Constituição nacional argentina pelo artigo 43, na forma de uma ação destinada a permitir o acesso a bancos de dados e a possibilitar controles em relação a dados falsos ou discriminatórios.[306] O *Habeas Data* argentino é aplicável tanto a bancos de dados públicos quanto privados. Igualmente, a Constituição nacional argentina contempla em seus artigos 18 e 19 a inviolabilidade do domicílio e da correspondência, bem como a privacidade da consciência pessoal.[307] Confira-se a redação dos referidos artigos constitucionais:[308]

> *Artículo 18 –* [...] *El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación.*
>
> *Artículo 19 – Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe.*
>
> *Artículo 43 –* [...] *Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión,*

[304] PALAZZI, 2002. p. 59.
[305] PALAZZI, 2002. p. 60.
[306] PALAZZI, 2002. pp. 62-63.
[307] PALAZZI, 2002. p. 139.
[308] ARGENTINA. **Constitución de la Nación Argentina**, 1994. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm. Acesso em: 2 nov. 2023.

> *rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística.*

Embora tais disposições não tenham estabelecido um direito constitucional explícito à proteção dos dados, a ação de *Habeas Data* permitiu a construção de uma jurisprudência na Argentina que abordou questões relacionadas ao tema. Em 1998, o caso *Facundo Urteaga* marcou a primeira vez que a Corte Suprema de Justiça da Argentina reconheceu aspecto que deu origem ao direito à proteção de dados,[309] ao firmar o *Habeas Data* como extensão do direito à privacidade e intimidade e permitir o acesso a dados de uma pessoa desaparecida a pedido de um familiar.[310-311] No decorrer do tempo, os tribunais também buscaram estabelecer princípios e direitos de proteção de dados por meio da ação de *Habeas Data*, mesmo na ausência de uma lei específica sobre o tema.

Para Johanna C. Faliero, o *Habeas Data* resultou na proteção tanto processual quanto material dos dados pessoais.[312] Nesse sentido, Pablo Palazzi afirma que, com a retificação e atualização dos dados, o *Habeas Data* criou direitos subjetivos, pois estava implícito em sua concepção que, se os indivíduos poderiam iniciar uma ação com base nesses motivos, eles teriam o direito de exigir a qualidade dos dados armazenados em registros públicos e privados.[313] Além do *Habeas Data*, certos tribunais recorreram a outros institutos, como o abuso de direito, ou a regras de proteção ao consumidor para tratar da temática de proteção de dados pessoais.[314]

2.3.1.1. A Lei Geral de Proteção de Dados argentina e regulamentos

À medida que a jurisprudência em torno do *Habeas Data* evoluiu, os debates em favor da criação de uma lei geral de proteção de dados e de uma regulamentação para a ação de *Habeas Data* intensificaram-se na Argentina. Além disso, a aprovação da

---

[309] MARTINÉZ, Esteban Ruiz. **Protección de los datos personales en los informes creditícios: delitos contra la intimidad informática**. Buenos Aires: Hammurabi. 2015, p. 61.

[310] ARGENTINA. Corte Suprema De Justicia De La Nación**, Urteaga, Facundo Raúl c/ Estado Nacional – Estado Mayor Conjunto de las FF.AA. – s/amparo Ley 16.986**. Buenos Aires: 1998. Disponível em: http://www.saij.gob.ar/corte-suprema-justicia-nacion-federal-ciudad-autonoma-buenos-aires-urteaga-facundo-raul-estado-nacional-estado-mayor-conjunto-ffaa-amparo-ley-16986-fa98001242-1998-10-15/123456789-242-1008-9ots-eupmocsollaf. Acesso em: 2 nov. 2023.

[311] TRAVIESO, Juan Antonio. **Régimen juridico de los datos personales. Hábeas data, cloud computing, responsabilidad, delitos, internet, redes, biometria**. Buenos Aires: Abeledo Perrot, 2014.

[312] FALIERO, Johanna C. La protección de los datos personales del consumidor y su importancia cardinal en nuestro sistema jurídico argentino. **Revista luso-brasileira de direito do consumo**, JM Editora, v. 7, n. 27, pp. 111-126, set. 2017.

[313] PALAZZI, 2002, p. 144.

[314] PALAZZI, 2002. p. 170.

Diretiva 95/46/CE também motivou a Argentina a buscar o desenvolvimento de uma legislação equivalente, especialmente diante da sua relação econômica com a Espanha.

Com base nesses antecedentes, a Argentina aprovou a Lei nº 25.326 na virada do milênio.[315] O marco legal da Argentina se destaca como uma das primeiras leis abrangentes de proteção de dados promulgadas na América Latina, que define, entre outras disposições, os princípios gerais de proteção de dados pessoais, os direitos dos titulares de dados, as obrigações para o tratamento de dados pessoais, a criação de uma autoridade responsável pela supervisão da proteção de dados e a regulamentação da ação de *Habeas Data*. A Lei nº 25.326/2000 dedicou uma seção exclusiva para tratar das transferências internacionais de dados pessoais, tema que será aprofundado no Capítulo3.

O objetivo da Lei nº 25.326/2000 se refere à proteção dos dados pessoais em arquivos, registros, bancos de dados ou outros meios técnicos de tratamento de dados, sejam eles públicos ou privados, destinados a fornecer informações, a fim de garantir o direito à honra e à intimidade de indivíduos, assim como o acesso às informações registradas que lhes dizem respeito. Conforme é evidenciado por esse objetivo, uma das particularidades da lei argentina é a importância atribuída aos registros em bases de dados, situação que decorre do período que antecedeu a disseminação da Internet, no qual os sistemas de informação se concentravam em bases de dados isoladas, muitas vezes sob o domínio do poder público.[316]

Em 2001, foi aprovado o Decreto nº 1558, com o intuito de regulamentar aspectos da Lei nº 25.326/2000 e esclarecer questões passíveis de interpretações divergentes.[317] Segundo Pablo Palazzi, a regulamentação das disposições referentes às transferências internacionais de dados refletiu interesses políticos e econômicos do país, na época.[318] O Decreto nº 1558/2001 introduziu hipóteses autorizadoras para a transferências de dados para países terceiros, em linha com a Diretiva 95/46/CE, de modo a favorecer o fluxo das informações com a UE. Além disso, o Decreto nº 1558/2001 possibilitou que entidades localizadas em países cuja proteção decorre de sistemas de autorregulação pudessem ser destinatárias dos dados transferidos da Argentina, o que permite reconhecer que os setores de países que não possuem uma lei que os regule, mas

[315] PALAZZI, 2002. p.139.
[316] REIGADA, 2012. pp. 30-31.
[317] ARGENTINA. Decreto nº 1558/2001**: apruébase la reglamentación de la Ley nº 25.326**. Disponível em: https://www.argentina.gob.ar/normativa/nacional/decreto-1558-2001-70368/actualizacion . Acesso em: 2 nov. 2023.
[318] PALAZZI, 2002. p. 166.

que se organizaram de maneira a proteger adequadamente os dados pessoais, podem ser destinatários de transferências provenientes da Argentina.

2.3.1.2. A Autoridade de Proteção de Dados Pessoais argentina

A APD da Argentina foi estabelecida pelo artigo 29 da Lei nº 25.326/2000, regulamentado pelo Decreto nº 1558/2001. Isso resultou na criação da *Dirección Nacional de Protección de Datos Personales* (DNPDP), que foi integrada, inicialmente, à estrutura do Ministério da Justiça, Segurança e Direitos Humanos. Nessa conjuntura, a DNPDP também exerceu a função de supervisionar questões relacionadas ao acesso à informação pública, tendo em vista a inexistência de legislação que instituísse um órgão de fiscalização para essa matéria. Em 2016, foi aprovada a Lei de Acesso à Informação Pública na Argentina (Lei nº 27.275/2016)[319] e determinada a criação da *Agencia de Acceso a La Información Pública* (AAIP) na forma de um organismo autárquico integrado à administração indireta do governo argentino. Pouco tempo depois, em 2017, a DNPDP passou fazer parte da AAIP e deixou de estar subordinada à administração direta, ampliando o seu grau de independência.[320]

A AAIP tem poderes para tomar as medidas necessárias para o cumprimento dos objetivos da Lei nº 25.326/2000, como editar regulamentos, investigar, intervir e sancionar. Com o decorrer do tempo, a AAIP emitiu regulamentos que normatizaram uma série de aspectos da Lei nº 25.326/2000, a exemplo das regras para regular transferência internacionais de dados para países terceiros, que serão examinados no Capítulo 3. Ainda, a AAIP tem o papel de fiscalizar instrumentos de autorregulação estabelecidos pela Lei nº 25.326/2000.

2.3.1.3. A Argentina nos cenários internacional e regional

A Argentina ganhou destaque no cenário internacional pelo seu conjunto de normas de proteção de dados. Pouco tempo depois da aprovação da Lei nº 25.326/2000, o Grupo de Trabalho Artigo 29 emitiu o Parecer nº 4 de 2002, que trata do nível de

---

[319] ARGENTINA. Ley 27.275/2016. **Derecho de Acesso a la Información Pública.** Honorable Congreso de la Nacion Argentina, 6 set. 2016. Disponível em: https://www.argentina.gob.ar/normativa/nacional/ley-27275-265949/actualizacion. Acesso em: 2 nov. 2023.

[320] SIMÃO, Bárbara; et al. **Autoridades de Proteção de Dados na América Latina: um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai**. São Paulo, IDEC, 2019. p.12. Disponível em: https://idec.org.br/publicacao/autoridade-de-protecao-de-dados-na-america-latina. Acesso em: 2 nov. 2023.

proteção conferido pela Argentina para a transferência de dados pessoais com a UE, conforme a Diretiva 95/46/CE.[321] Nessa ocasião, o Grupo expressou a preocupação de que a incorporação da DNPDP à estrutura do Ministério poderia não garantir a sua plena independência para atuação. Essa teria sido a principal motivação para a reforma institucional que incorporou a DNPD à AAIP anos depois.[322] A despeito disso, a opinião do Grupo foi de que a Argentina teria nível adequado de proteção com os padrões europeus.

Em 2003, a Comissão Europeia realizou a avaliação do regime de proteção da Argentina para receber dados pessoais transferidos a partir da UE sob a Diretiva 95/46/CE.[323] A Comissão constatou que a Constituição nacional argentina, a Lei nº 25.326/2000 e o Decreto nº 1558/2001, constituem o arcabouço de proteção de dados do país. No âmbito das garantias constitucionais, foi ressaltado que o *Habeas Data* representa tanto um meio de reparação judicial especial para a proteção de dados pessoais reconhecido pela jurisprudência argentina e como um direito fundamental aplicável.

Nessa esteira, a Comissão indicou que a Lei nº 25.326/2000 e o seu decreto regulamentador teriam alargado as disposições constitucionais e incluído medidas relacionadas aos princípios gerais de proteção de dados, os direitos dos titulares, as obrigações dos responsáveis pelo tratamento dos dados, as funções da autoridade administrativa de supervisão, além de sanções e regras processuais relativas à reparação judicial da ação de *Habeas Data*. A Comissão considerou que a Argentina assegura nível adequado de proteção dos dados pessoais. A partir desse marco, a Argentina se tornou o primeiro país latino-americano a ter o respaldo de uma decisão de adequação para recepcionar dados pessoais transferidos a partir da UE. Até o momento, não houve reconsideração sob a vigência do RGPD.

A Argentina igualmente se sobressaiu no cenário internacional de proteção de dados com a ratificação da Convenção 108 do Conselho da Europa. A iniciativa para adesão a esse convênio teria iniciado após a aprovação da Lei nº 25.326/2000, mas não emplacou devido à falta de independência plena da DNPDP na época. Com a criação da

---

[321] UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Opinion 4/2002 on the level of protection of personal data in Argentina (11081/02/EN/Final WP 63)**. Bruxelas, 3 out. 2002. Disponível em:https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm. Acesso em: 2 nov. 2023.

[322] SIMÃO, et al, 2019. p. 12.

[323] COMISSÃO EUROPEIA. **Decisão da Comissão nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais na Argentina** (2003/490/CE). Bruxelas, 3 jun. 2003**.** Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003D0490. Acesso em: 2 nov. 2023.

AAIP, a adesão da Argentina à Convenção 108 foi aprovada em 2019. A Argentina também ratificou, em 2023, a atualização do Conselho da Europa na forma da Convenção 108+.[324] Esse movimento foi destacado, pela AAIP, como crucial para a agenda de proteção de dados do país diante do crescimento exponencial de transformações tecnológicas.[325] Além disso, a Argentina se somou à Convenção de Budapeste, em 2018, e assinou seu Segundo Protocolo Adicional, em 2023, para endereçar crimes cibernéticos.

A participação da Argentina na região latino-americana também é evidente. O país integra o Comitê Executivo da RIPD, que, entre outras funções, é responsável por aprovar o programa de trabalho da Rede, organizar sessões, engajar-se em eventos e aprovar a constituição de grupos de trabalho.[326] Ainda, a Argentina está envolvida nas ações da Agenda Digital do Mercosul, entre as quais resultou o Acordo sobre o Comércio Eletrônico do bloco.[327]

2.3.1.4. Propostas de modernização da Lei de Proteção de Dados argentina

A Lei nº 25.326/2000, que esteve à frente da vanguarda da proteção de dados pessoais na América Latina, tem sido considerada desatualizada, após os 23 anos de sua promulgação. Essa avaliação surge, principalmente, devido à rápida evolução das tecnologias, que causaram impactos notáveis na privacidade de indivíduos e, atualmente, demandam abordagens renovadas para lidar com os riscos associados à segurança dos dados pessoais. Além disso, as mudanças no âmbito internacional, notadamente com a implementação do RGPD, acentuaram a necessidade de atualização da legislação argentina, especialmente para que o país preservasse o seu status internacional de proteção de dados.

Em 2017, um esforço conjunto do Ministério da Justiça, Segurança e Direitos Humanos com a AAIP, denominado de *Justicia 2020,* sugeriu modificações à Lei nº 25.326/2000. O projeto resultante foi apresentado ao Poder Legislativo, em 2018.

---

[324] CONSELHO DA EUROPA. Convention 108. **Treaty list for a specific State – Argentina**. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaties-full-list-signature&CodePays=ARG. Acesso em: 2 nov. 2023.

[325] AAIP. **La titular de la AAIP depositó en representación de la Argentina el instrumento de ratificación del convenio 108+**. 18 mar. 2023(c). Disponível em: https://www.argentina.gob.ar/noticias/la-titular-de-la-aaip-deposito-en-representacion-de-la-argentina-el-instrumento-de. Acesso em: 2 nov. 2023.

[326] REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. **Órganos de la Red Iberoamericana de Protección de Datos**. 2023. Disponível em: https://www.redipd.org/es/la-red/organos-de-la-red-iberoamericana-de-proteccion-de-datos. Acesso em: 2 nov. 2023.

[327] MERCOSUL. **Agenda Digital**. 2023. Disponível em: https://www.mercosur.int/pt-br/temas/agenda-digital/. Acesso em: 2 nov. 2023.

Entretanto, ao longo dos últimos anos, a iniciativa perdeu apoio e o projeto não obteve êxito.[328] Apesar desse revés, em 2022, a AAIP divulgou um novo projeto de lei de proteção de dados pessoais (Projeto de Lei da AAIP), com o intuito de substituir a Lei nº 25.326/2000.[329] A nova estrutura legal possui propostas de atualização similares ao projeto de 2018 e busca enfrentar os desafios emergentes da transformação tecnológica e do desenvolvimento da economia digital.

Na elaboração do Projeto de Lei da AAIP, foram considerados padrões, recomendações e princípios internacionais e regionais, incluindo o RGPD, a Convenção 108+ do Conselho da Europa, os Padrões de Proteção de Dados Pessoais emitidos pela RIPD, bem como leis de países latino-americanos, como a LGPD do Brasil. Para fomentar o debate amplo com a sociedade civil, a academia, o setor privado econômico e o setor público, a AAIP submeteu o projeto à consulta pública.[330] Após a incorporação das contribuições multissetoriais recebidas nessa ocasião, o Projeto de Lei da AAIP foi encaminhado aos Poderes Executivo e Legislativo da Argentina, para considerações e está em processo de discussão.[331]

2.3.2. Uruguai

A Constituição do Uruguai, de 1967, contempla em seus artigos 10 e 28 a proteção da privacidade da consciência pessoal, bem como a inviolabilidade de documentos particulares e da correspondência. O artigo 72 protege uma gama de garantias e direitos intrinsecamente ligados à natureza da personalidade humana, mesmo que não estejam especificados no texto constitucional. Já o artigo 332 estabelece que a ausência de previsão legal para a proteção de direitos pode ser suprida por meio de fundamentos

---

328 AAIP. **Ley de protección de los datos personales en Argentina: sugerencias y aportes recibidos en lo proceso de reflexión sobre la necesidad de su reforma**, ago. 2017. p. 40. Disponível em: https://www.argentina.gob.ar/sites/default/files/documento_aportes_reforma_ley25326_0.pdf. Acesso em: 2 nov. 2023.

329 AAIP. **Informe sobre el proceso de Elaboración Participativa de Normas en relación al anteproyecto de Ley de Protección de Datos Personales**, out. 2022. p 33. Disponível em: https://www.argentina.gob.ar/sites/default/files/informe_consulta_publica_aaip_pdf. Acesso em: 2 nov. 2023.

330 AAIP. **Presentación del Proyecto de Ley de Protección de Datos Personales**, nov. 2022(b). Disponível em: https://www.argentina.gob.ar/noticias/presentacion-del-proyecto-de-ley-de-proteccion-de-datos-personales. Acesso em: 2 nov. 2023.

331 AAIP. **Proyecto de Ley de Protección de Datos Personales**, out. 2022(c). p. 45. Disponível em: https://www.argentina.gob.ar/sites/default/files/proyecto_de_ley_de_datos_personales_aaip.pdf. Acesso em: 2 nov. 2023.

de leis análogas, de princípios gerais do direito e da doutrina amplamente aceita. Confira-se a redação dos referidos artigos constitucionais:[332]

> *Artículo 10 – Las acciones privadas de las personas que de ningún modo atacan el orden público ni perjudican a un tercero, están exentas de la autoridad delos magistrados. Ningún habitante de la República será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe.*
>
> *Artículo 28 – Los papeles de los particulares y su correspondencia epistolar, telegráfica o de cualquier otra especie, son inviolables (...).*
>
> *Artículo 72 – La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno.*
>
> *Artículo 332 – Los preceptos de la presente Constitución que reconocen derechos a los individuos, así como los que atribuyen facultades e imponen deberes a las autoridades públicas, no dejarán de aplicarse por falta de la reglamentación respectiva, sino que ésta será suplida, recurriendo a los fundamentos de leyes análogas, a los principios generales de derecho y a las doctrinas generalmente admitidas.*

Com base nos artigos 72 e 332, é reconhecido que a Constituição do Uruguai permite apresentar todas as ações e garantias necessárias para a tutela de aspectos inerentes à personalidade humana.[333] Segundo Marcelo Bauzá, os direitos intrínsecos à condição humana não se impõem somente ao legislador, mas também ao constituinte, uma vez que são preexistentes à organização estatal.[334] Assim, ainda que não haja menção explícita ao direito à proteção de dados na Constituição uruguaia, nem a incorporação expressa do *Habeas Data*, esses direitos são reconhecidos como direitos fundamentais.[335]

2.3.2.1. A Lei Geral de Proteção de Dados uruguaia e regulamentos

Ainda na década de 1990, foram apresentados diversos projetos de lei aos órgão legislativo do Uruguai que tratavam de proteção de dados pessoais, porém essas propostas se concentravam em questões de dados de crédito.[336] Em 2004, foi sancionada a Lei nº 17.838, intitulada de *Ley de Protección de Datos Personales para ser utilizados en Informes Comerciales y Acción de Hábeas Data*, que tinha como objetivo a proteção de dados pessoais para fins comerciais.[337] A Lei nº 17.838/2004 estabeleceu pela primeira

---

[332] URUGUAI. **Constitución de la Republica**, 1967. Disponível em: https://parlamento.gub.uy/documentosyleyes/constitucion. Acesso em: 2 nov. 2023.
[333] GUADAGNA; BRACESCO, 2010. pp. 335-336.
[334] BAUZÁ, Marcelo. **Manual de derecho informático e informática jurídica II.** Montevideo: Fundación de Cultura Universitaria, 2018. p. 15.
[335] PALAZZI, 2002. p. 93.
[336] PALAZZI, 2002. p. 93.
[337] URUGUAI. **Ley 17.838/2004 de Protección de Datos Personales para ser utilizados en Informes Comerciales y Acción de Hábeas Data**. 24 set. 2004. Disponível em: https://www.impo.com.uy/bases/leyes-originales/17838-2004. Acesso em: 2 nov. 2023.

vez um arranjo legal para o *Habeas Data* ao referir-se às pretensões de conhecer, corrigir, atualizar e suprimir dados pessoais.[338]

Apesar dos avanços na proteção de dados pessoais no âmbito comercial, a necessidade de incorporar uma proteção mais ampla no ordenamento jurídico uruguaio se tornou evidente com os crescentes desafios tecnológicos e o desenvolvimento de iniciativas eletrônicas no governo do país.[339] Atrelado a isso, a aprovação de uma lei geral de proteção de dados pessoais à luz dos padrões europeus era vista como meio de se buscar o reconhecimento da UE para a transferência de dados pessoais, bem como de atrair oportunidades de negócio e investimento nos setores de tecnologia e serviço.[340]

Nesse contexto, a *Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento* (AGESIC), juntamente com as contribuições fornecidas pelo *Instituto de Derecho Informático* (IDI), da Faculdade de Direito de UDELAR, e pelo Órgão de Controle do Ministério de Economia e Finanças, apresentou anteprojeto para instituição de um marco legal de proteção de dados no Uruguai.[341]A partir desses antecedentes, a Lei nº 18.331 foi sancionada em 2008, revogando expressamente o regime estabelecido na antiga Lei nº 17.838/2004.

A Lei nº 18.331/2008 esclarece o entendimento segundo o qual o direito à proteção de dados pessoais é inerente à natureza humana e está abrangido pelo artigo 72 da Constituição. Tendo como referência a Diretiva 95/46/CE e a lei espanhola de proteção de dados, além da experiência Argentina na região, a Lei nº 18.331/2008 delineou, entre outros aspectos, os princípios de proteção de dados pessoais, os direitos de titulares dos dados, as obrigações relacionadas a bases de dados de titularidade pública e privada, a autoridade administrativa responsável por supervisionar a aplicação da norma e o instrumento de *Habeas Data*, por meio da qual o titular dos dados pode intentar ação judicial contra o responsável pelo tratamento para exercer o direitos de acesso, retificação e supressão de seus dados pessoais.[342] A Lei nº 18.331/2008 reservou uma seção

---

[338] GUADAGNA; BRACESCO, 2010. p. 338.

[339] SARASOLA, Florencia. **Ley de Protección de Datos Personales**. Universidad ORT Uruguay, Facultad de Ingeniería. Montevidéu, 2009. Disponível em: https://silo.tips/download/ley-de-proteccion-de-datos-personales-3. Acesso em: 2 nov. 2023.

[340] SARASOLA, 2009. p. 7.

[341] SARASOLA, 2009. p. 8.

[342] BORCHE, Alejandro; SENA, Sonia. Incidencia de las leyes de protección de datos y acceso a la información pública en la gestión de la administración. **V Encontro Internacional do CONPEDI** Montevidéu, 2016. Disponível em:http://site.conpedi.org.br/publicacoes/9105o6b2/za57d3t3/sX1aUAW7kQ8nG1D9.pdf. Acesso em: 2 nov. 2023

específica para abordar as transferências internacionais de dados pessoais, assunto que será detalhado no Capítulo 3.

Com o decorrer do tempo, as disposições contidas na Lei nº 18.331/2008 foram regulamentadas por decretos. O Decreto nº 414, de 2009, esclareceu conceitos fundamentais, além de regular a organização, os poderes e o funcionamento da autoridade administrativa de supervisão.[343] O preâmbulo desse Decreto destaca a conveniência da adaptação da legislação uruguaia ao regime de direito consagrado pelos países europeus por meio da Diretiva 95/46/CE. Nessa direção, o Uruguai vem se empenhando de forma contínua para atualizar a sua legislação de proteção de dados à luz dos desenvolvimentos da UE.

Esse é o caso da Lei 19.670, de 2018, e do Decreto nº 64 de 2020, que introduziram modificações recentes à Lei nº 18.331/2008 com base em elementos típicos do RGPD, a exemplo da ampliação da lei uruguaia para tutelar situações extraterritoriais e de contornos para o denominado princípio da responsabilidade proativa.[344-345] O preâmbulo do referido decreto reconhece que a ubiquidade de indivíduos no mundo digital e a salvaguarda de seus direitos requerem atenção especial quanto ao alcance da proteção de suas dados pessoais, que deve ser complementada por meio de mecanismos de controle de conformidade em nível global e pela atribuição de responsabilidades ao agentes, ainda que estejam localizados fora do território uruguaio.

Cabe observar que a proteção de dados pessoais e o acesso a informações públicas são temas que caminharam de maneira conjunta no Uruguai.[346] A aprovação da Lei nº 18.381, em 2008, sob o título *Ley sobre el Derecho de Acceso a la Informacion Publica*, logo após a promulgação da sua lei de proteção de dados, é um reflexo da importância desses tópicos no cenário jurídico do país.[347] Sob a perspectiva regulatória,

---

343 URUGUAI: **Decreto 414/2009: reglamentacion de la Ley 18.331. Relativo a la Proteccion de Datos Personales**. 5 out. 2009. Disponível em: https://www.impo.com.uy/bases/decretos/414-2009. Acesso em: 2 nov. 2023.

344 URUGUAI. Ley 19.670/2018: **aprobación de rendición de cuentas y balance de ejecución presupuestal.** Registro Nacional de Leyes y Decretos. 25 out. 2018. Disponível em: https://www.impo.com.uy/bases/leyes/19670-2018. Acesso em: 2 nov. 2023.

345 URUGUAI. **Decreto 64/2020: reglamentación de los arts. 37 a 40 de la Ley 19.670 y art. 12 de la Ley 18.331/2008 a proteccion de datos personales**. Registro Nacional de Leyes y Decretos. 21 fev. 2020. Disponível em: https://www.impo.com.uy/bases/decretos/64-2020. Acesso em: 2 nov. 2023.

346 BORCHE; SENA, 2016. p. 141.

347 URUGUAI. **Ley 18.381/2008: sobre el Derecho de Acceso a la Informacion Publica**. Registro Nacional de Leyes y Decretos. 7 nov. 2008. Disponível em: https://www.impo.com.uy/bases/leyes/18381-2008/9. Acesso em: 2 nov. 2023.

as unidades de controle em matérias de proteção de dados e de acesso à informação integram conjuntamente a estrutura organizacional da AGESIC.

2.3.2.2. A Autoridade de Proteção de Dados Pessoais uruguaia

A APD do Uruguai foi criada pelo artigo 31 da Lei nº 18.331/2008 e é conhecida como *Unidad Reguladora y de Control de Datos Personales* (URCDP). Do ponto de vista organizacional, a URCDP está localizada no âmbito da estrutura da AGESIC, que, por sua vez, é um órgão vinculado à Presidência da República.[348] A AGESIC tem como principais objetivos propor a formulação de políticas em relação à sociedade da informação e ao conhecimento, promover o melhor uso das TIC no país, estabelecer e propor normas, padrões e procedimentos técnicos em assuntos de informática, planejar e executar projetos do governo eletrônico com ênfase na melhoria dos serviços aos cidadãos, além de fiscalizar e auditar o cumprimento da regulamentação vigente em sua área de competência.[349]

A relação entre a AGESIC e a URCDP é de desconcentração administrativa, o que significa que a URCDP possui competência própria e autonomia técnica determinada por lei, mas mantem-se subordinada à administração direta do governo uruguaio por estar integrada à estrutura da AGESIC.[350] Cabe destacar que a *Unidad de Acceso a la Información Pública* (UAIP) também constitui órgão desconcentrado da AGESIC. A URCDP tem poderes normativos, de investigação e sanção para resolver matéria de proteção de dados. Ao longo de sua atuação, a URCPD emitiu uma variedade de orientações que oferecem diretrizes sobre a aplicação eficaz da Lei nº 18.331/2008 e incluem os regulamentos sobre as hipóteses de transferência internacionais de dados para países terceiros, que serão examinados no Capítulo 3. Recentemente, a URCDP publicou o Guia Geral de Proteção de Dados do Uruguai, de 2022, que fornece um resumo abrangente do marco legal e das suas subsequentes atualizações.[351]

---

[348] BORCHE; SENA, 2016. p. 132.
[349] BORCHE; SENA, 2016. pp.132-133.
[350] SIMÃO et al, 2019. p. 29.
[351] URCDP.**Guía general de Protección de Datos Personales en Uruguay**, 24 jan. 2022. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-general-proteccion-datos-personales-uruguay. Acesso em: 2 nov. 2023.

2.3.2.3. O Uruguai nos cenários internacional e regional

Assim como a Argentina, o Uruguai se sobressaiu no cenário internacional de proteção de dados pessoais pelo seu conjunto de normas de proteção de dados. Ainda sob a égide da Diretiva 95/46/CE, o Grupo de Trabalho Artigo 29 emitiu o Parecer nº 6, de 2010, sobre o nível de proteção conferido pelo Uruguai para a transferência de dados pessoais com a UE.[352] Nessa oportunidade, as autoridades uruguaias puderam esclarecer que a Lei nº 18.331/2008 é aplicável supletivamente às leis especiais que regem bases de dados do país, por força da cláusula aberta prevista no artigo 332 da Constituição. De forma geral, a avaliação conduzida pelo Grupo não identificou aspectos de preocupação substanciais, o que refletiu positivamente na opinião de que o Uruguai garante nível adequado de proteção.

No ano de 2012, a Comissão Europeia conduziu a análise do regime de proteção de dados do Uruguai para recepcionar dados pessoais provenientes da UE, nos termos da Diretiva 95/46/CE.[353] A Comissão destacou que a Constituição uruguaia, a Lei nº 18.331/2008 e o Decreto nº 414/009, além de instrumentos internacionais dos quais o Uruguai é signatário, como a Convenção Americana de Direitos Humanos (Pacto de São José da Costa Rica), compreendem a estrutura de proteção de dados do país. Da mesma forma, foi pontuado que o Uruguai foi convidado a ratificar a Convenção 108 do Conselho da Europa.

Com relação aos preceitos da Constituição uruguaia, a Comissão destacou que a enumeração dos direitos fundamentais não constitui uma lista fechada, considerando que o artigo 72 da Constituição determina que a lista de direitos, obrigações e garantias previstos no texto constitucional não exclui outros que sejam inerentes à personalidade humana ou que derivem da forma republicana de governo. Quanto às normas de proteção dos dados pessoais do Uruguai, a Comissão reconheceu que as disposições da lei uruguaia se baseiam em grande medida nas normas da Diretiva 95/46/CE, cobrindo os princípios básicos necessários para assegurar um nível adequado

---

[352] UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay (0475/10/EN WP 177).** Bruxelas, 12 out. 2010. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp177_en.pdf. Acesso em: 2 nov. 2023.

[353] COMISSÃO EUROPEIA. **Decisão da Comissão nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados** (2012/484/UE). Bruxelas, 12 ago. 2012**.** Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012D0484. Acesso em: 2 nov. 2023.

de proteção e prevendo exceções e limitações de modo a salvaguardar interesses públicos relevantes. A Comissão também assinalou que aplicação da lei é garantida por meio de recursos administrativos e judiciais, em especial pela ação de *Habeas Data*, e do controle efetuado pela URCDP. Nesse sentido, a Comissão considerou que o Uruguai assegura nível adequado de proteção de dados pessoais. Assim como no caso da Argentina, não houve reconsideração sob a vigência do RGPD até o momento e o Uruguai vem envidando esforços para manter a sua legislação alinhada aos padrões adotados pela UE para perseverar o seu status internacional.

Como indicado na decisão de adequação da Comissão Europeia, o Uruguai foi convidado a integrar o grupo de países signatários da Convenção 108 do Conselho da Europa em resposta ao interesse manifestado pelo país em 2011. O Comitê Consultivo considerou que o Uruguai adotou as medidas necessárias em sua legislação doméstica para dar efeito aos princípios básicos de proteção de dados da Convenção.[354] Assim, em 2013, o Uruguai se tornou o primeiro país não europeu a aderir ao instrumento, abrindo caminho para outras nações situadas além das fronteiras europeias, como a Argentina.[355] A Convenção 108+ foi ratificada pelo Uruguai em 2021.[356]

Mais recentemente, o Uruguai também recebeu um convite para se unir à Convenção de Budapeste em correspondência à solicitação efetivada em 2022. O Ministério das Relações Exteriores do Uruguai vem trabalhando em colaboração com outras instituições nacionais competentes na área para avançar na adesão do país à Convenção.[357] No contexto latino-americano, o Uruguai tem se destacado por seu envolvimento nas iniciativas regionais relacionadas à proteção de dados e

[354] CONSELHO DA EUROPA. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Request by Uruguay to be invited to accede**, 2011. Disponível em: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cce94. Acesso em: 2 nov. 2023.

[355] CONSELHO DA EUROPA. **Convention 108. Treaty list for a specific State – Uruguay**. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaties-full-list-signature&CodePays=URU. Acesso em: 2 nov. 2023.

[356] URCDP. **Nueva ley que aprueba el Convenio 108+**. 9 abr. 2021. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/noticias/nueva-ley-aprueba-convenio-108. Acesso em: 2 nov. 2023.

[357] URUGUAI. Ministerio de Relaciones Exteriore. **Uruguay es invitado por el Consejo de Europa a adherir al Convenio de Budapest sobre Ciberdelincuencia**. 14 fev. 2023 Disponível em: https://www.gub.uy/ministerio-relaciones-exteriores/comunicacion/comunicados/uruguay-es-invitado-consejo-europa-adherir-convenio-budapest-sobre. Acesso em: 2 nov. 2023.

desenvolvimento digital. O país integra o Comitê Executivo da RIPD[358] e atua nas ações da Agenda Digital do Mercosul.[359]

2.3.3. Colômbia

A Constituição da Colômbia, de 1991, introduziu em seu artigo 15 o direito à intimidade e o direito de conhecer, atualizar e retificar informações coletadas sobre indivíduos em bancos de dados ou em arquivos de entidades públicas e privadas. Esse dispositivo igualmente estabelece que a liberdade e outras garantias constitucionais devem ser respeitadas na coleta, no tratamento e na circulação de dados, além de determinar a inviolabilidade da correspondência e das comunicações privadas. Já o artigo 20 refere-se à liberdade de expressão, de informar e de receber informação. Confira-se a redação dos referidos artigos constitucionais:[360]

> *Artículo 15 – Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.*
>
> *En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.*
>
> *La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley (...).*
>
> *Artículo 20 – Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.*
>
> *Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.*

No decorrer da Assembleia Nacional Constituinte, ocorreram debates sobre o uso do termo *Habeas Data* como referência aos direitos de conhecimento, atualização e retificação de informações. Embora o instituto não tenha sido explicitamente incorporado ao texto final, as discussões entre os constituintes produziram efeitos, uma vez que, posteriormente, o *Habeas Data* foi associado à ação de tutela por meio do Decreto nº 2591 de 1991.[361]

---

[358] REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. **Órganos de la Red Iberoamericana de Protección de Datos**. 2023. Disponível em: https://www.redipd.org/es/la-red/organos-de-la-red-iberoamericana-de-proteccion-de-datos. Acesso em: 2 nov. 2023.

[359] MERCOSUL. **Agenda Digital**. 2023. Disponível em: https://www.mercosur.int/pt-br/temas/agenda-digital/. Acesso em: 2 nov. 2023.

[360] COLOMBIA. **Constitución Politica de Colombia**, 1991. Disponível em: https://dapre.presidencia.gov.co/normativa/constitucion-politica. Acesso em: 2 nov. 2023.

[361] REMOLINA, 2015. pp. 130-132.

A ação de tutela é um instrumento processual previsto no artigo 86 da Constituição colombiana que visa a garantir a proteção imediata de direitos fundamentais. Qualquer cidadão tem o direito de apresentar a ação perante um magistrado com o intuito de obter uma ordem para que a parte contra a qual a tutela é requerida adote uma ação ou se abstenha de agir. A decisão deve ser encaminhada à Corte Constitucional colombiana, que poderá revisá-la, caso considere pertinente. O Decreto nº 2591/1991, ao regulamentar a conduta de particulares, estabelece que a ação de tutela é aplicável quando dirigida à entidade privada contra a qual foi feito o pedido no exercício de *Habeas Data*, conforme determinado pelo artigo 15 da Constituição.[362] Com essa redação, o Decreto nº 2591/1991 esclareceu que os direitos estabelecidos no artigo 15 se referem ao *Habeas Data*.

Da mesma forma, o *Habeas Data* foi reconhecido pela jurisprudência da Corte Constitucional da Colômbia, que emitiu uma série decisões no decorrer dos anos a respeito do seu escopo e características, bem como das condições necessárias para o tratamento de dados pessoais.[363] A Corte Constitucional da Colômbia possui três categorias de sentenças. Primeiro, a Sentença T (Tutela) trata de violações a direitos fundamentais, geralmente com efeitos *interpartes*. Segundo, a Sentença U (Unificada) unifica decisões de tutela provenientes de instâncias inferiores, produzindo efeitos *erga omnes*. Terceiro, a Sentença C (Constitucional) avalia a conformidade das leis com a Constituição, de modo a interpretar, esclarecer e até revogar eventuais disposições.[364]

A Sentença T-414, de 1992, foi a primeira a tratar do direito ao *Habeas Data*.[365] De início, esse direito foi compreendido pela Corte como uma garantia do direito à intimidade, na qual se considerou a proteção dos dados dentro da esfera da vida privada e familiar, onde nem o Estado, nem particulares podem interferir.[366] Mais tarde, o direito ao *Habeas Data* foi interpretado pela Corte como uma manifestação do livre desenvolvimento da personalidade e da autodeterminação informativa do indivíduo.[367]

---

[362] COLOMBIA. Decreto nº 2591/1991**: por el cual se reglamenta la acción de tutela consagrada en el artículo 86 de la Constitución Política 1991**. Función Pública, 1991. Disponível em: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=5304. Acesso em: 2 nov. 2023.

[363] REMOLINA, Nelson. ¿ Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?. **International Law**, n. 16, 2010. pp. 489-523.

[364] BLANCO GAITAN, David. Challenges of Colombian Data Protection Framework Towards a European Adequate Level of Protection. **University of Oslo**, 2019. Disponível em: https://www.duo.uio.no/handle/10852/68578. Acesso em: 2 nov. 2023.

[365] ROJAS BEJARANO, Marcela. Evolución del derecho de protección de datos personales en colombia respecto a estándares internacionales. **Novum Jus**, 8 (1), 2014, pp. 107-139. Disponível em: https://repository.ucatolica.edu.co/entities/publication/b8054942-c619-46cc-8e58-46039f6ec2b6. Acesso em: 2 nov. 2023.

[366] ROJAS BEJARANO. 2014. p. 120.

[367] ROJAS BEJARANO. 2014. p. 121.

Em última análise, o direito ao *Habeas Data* passou a ser considerado um direito autônomo, cujo núcleo essencial refere-se às faculdades de conhecer, atualizar e retificar informações que tenham sido coletadas em bancos de dados e arquivos de entidades públicas e privadas, nos termos do artigo 15 da Constituição.[368]

2.3.3.1. A Lei Geral de Proteção de Dados colombiana e regulamentos

A construção da jurisprudência da Corte Constitucional colombiana desenvolveu uma série de fundamentos e princípios para a coleta, armazenamento e uso de dados pessoais.[369] A atuação da Corte, portanto, preparou terreno para a proposição de marcos legais voltados à proteção de dados na Colômbia. Após intensos debates, sobretudo de agentes ligados ao sistema financeiro, foi promulgada a Lei nº 1266 de 2008, que estabelece disposições sobre o *Habeas Data* e regula o tratamento de dados contidas em bases de dados, especialmente financeiras, creditícias e comerciais.[370] O escopo de proteção da Lei nº 1266/2008 está limitado à gestão de dados comerciais ou financeiros, destinados a calcular riscos creditícios. O caráter setorial da Lei nº 1266/2008 é reconhecido pela Corte Constitucional e por entidades públicas, como a Superintendência Financeira e a Superintendência de Indústria e Comércio.[371]

A insuficiência da Lei nº 1266/2008 provocou discussões em defesa da criação de normas mais abrangentes para a proteção de dados pessoais, alinhadas à jurisprudência que vinha sendo consolidada pela Corte Constitucional colombiana. Além disso, a adoção de uma lei geral de proteção de dados era fundamental para que a Colômbia pudesse alcançar um nível adequado de proteção perante as autoridades europeias, além de oferecer um quadro legal atrativo para atividades comerciais que envolvessem o tratamento de dados pessoais.[372]

Nesse sentido, em 2012, foi aprovada a Lei nº 1581, com o intuito de estabelecer disposições gerais para a proteção de dados pessoais e desenvolver o direito constitucional consagrado pelo *Habeas Data*. Tendo como referência a Diretiva

---

[368] ROJAS BEJARANO. 2014. p. 122.
[369] REMOLINA, 2015. p. 139.
[370] COLOMBIA. Ley Estatutaria 1.266/2008**: por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones**. 31 dez. 2008. Disponível em: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488. Acesso em: 2 nov. 2023.
[371] REMOLINA, 2010. p. 511.
[372] REMOLINA, 2015. pp. 135-136.

95/46/CE, a Lei nº 1.581/2012 prevê, entre outros, os princípios de proteção de dados, os direitos e condições para o tratamento de dados, as obrigações para os responsáveis pelo tratamento e a autoridade responsável pela sua supervisão. A Lei nº 1.581/2012 destinou um capítulo específico para tratar das transferências internacionais de dados pessoais, tema que será explorado no Capítulo 3.

Cabe destacar que esse texto legal deve ser aplicado e interpretado em harmonia com a Sentença C-748 de 2011 da Corte Constitucional,[373] que foi emitida como resultado da revisão de constitucionalidade.[374] Da mesma forma, o Decreto nº 1377 de 2013 regulamenta, parcialmente, aspectos da Lei nº 1.581/2012, tais como o consentimento e o exercício dos direitos dos titulares, as transferências e a transmissão de dados pessoais e o denominado princípio da responsabilidade demonstrada frente ao tratamento de dados.[375]

Ainda que a Colômbia tenha se juntado ao grupo de países latino-americanos que possuem lei abrangente de proteção de dados, a Lei setorial nº 1266/2008 permanece em vigor até hoje. [376] Recentemente, esse diploma foi atualizado pela Lei nº 2157, de 2021.[377] As principais modificações incluem garantias para os indivíduos, como a vedação ao uso de dados financeiros, registros de crédito e informações comerciais para a tomada de decisões empregatícias e, ainda, a impossibilidade de que consultas frequentes ao histórico de crédito sejam consideradas como um fator para reduzir a classificação de crédito de indivíduos.

---

[373] COLOMBIA. Corte Constitucional. **Sentencia C-748/11. Proyecto de Ley Estatutaria de Habeas Data y Proteccion de Datos Personales. Control De Constitucionalidad de Los Proyecto de Ley Estatutaria**, 2011. Disponível em: http://www.secretariasenado.gov.co/senado/basedoc/c-748_2011.html#inicio. Acesso em: 2 nov. 2023.

[374] REMOLINA, 2015. pp. 142-143.

[375] COLOMBIA. Decreto 1.377/2013**: por el cual se reglamenta parcialmente la Ley 1581 de 2012**. 27 Jun. Disponível em: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646. Acesso em: 2 nov. 2023.

[376] CANO, Lucero Galvis. El Panóptico digital de la protección de datos personales en Colombia. **Revista Temas**: Departamento de Humanidades Universidad Santo Tomás Bucaramanga, n. 12, 2018. pp. 125-140.

[377] COLOMBIA. Ley 2157/2021**: por medio de la cual se modifica y adiciona la Ley Estatutaria 1266 De 2008, y se dictan disposiciones generales del Habeas Data con relación a la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.** 29 out. 2021. Disponível em: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=173246. Acesso em: 2 nov. 2023.

2.3.3.2. Autoridade de Proteção de Dados Pessoais colombiana

Como analisado acima, a Corte Constitucional da Colômbia ocupa papel de destaque na interpretação da legislação de proteção de dados, sendo reconhecida como uma das cortes mais ativas na matéria constitucional na América Latina. Sua atuação no decorrer dos anos estabeleceu precedentes importantes que moldaram a forma como a proteção de dados é entendida no país. Além disso, atualmente, a aplicação do aparato legal de proteção de dados colombiano está sujeita à autoridade administrativa designada para exercer o controle e a supervisão das entidades responsáveis pelo tratamento de dados pessoais.[378]

O artigo 19 da Lei nº 1.581/2012 atribuiu essa competência à Superintendência de Indústria e Comércio (SIC) por meio da criação da *Delegatura de la Protección de Datos*, cuja função é assegurar o cumprimento efetivo dos princípios, direitos, garantias e procedimentos previstos na norma. A SIC compõe a administração indireta do Poder Executivo da Colômbia, sendo o órgão regulador responsável por outras matérias, como propriedade industrial, proteção do consumidor e defesa da concorrência.[379] Cabe à Superintendência Financeira a competência para regular a proteção de dados creditícios e financeiros, podendo a SIC intervir residualmente no assunto. Diante do acúmulo de competências da SIC, seu modelo é frequentemente comparado à FTC, nos EUA.[380]

A Lei nº 1.581/2012 permite que a SIC regulamente a legislação de proteção de dados colombiana, bem como imponha sanções aos responsáveis pelo tratamento de dados que não cumprem as obrigações estabelecidas. Além disso, a SIC tem poderes para solicitar a colaboração de entidades internacionais ou estrangeiras quando os direitos dos titulares forem afetados fora do território colombiano. A Circular Única da SIC tem como objetivo reunir em um único corpo normativo todas as regulamentações e instruções gerais emitidas pela autoridade. Em 2022, a SIC publicou a versão atualizada do Título V da Circular Única, dedicado à proteção de dados, que fornece diretrizes adicionais sobre o direito ao *Habeas Data* para informações financeiras e creditícias, o Registro Nacional de Bases de Dados e as transferências internacionais de dados pessoais, que serão examinadas no Capítulo 3.

[378] ROJAS BEJARANO, 2014. pp. 119-120.
[379] SIMÃO et al, 2019. p. 22.
[380] SIMÃO et al, 2019. p. 22.

2.3.3.3. A Colômbia nos cenários internacional e regional

Diferentemente da Argentina e do Uruguai, a Colômbia não conta com uma decisão de adequação da Comissão Europeia para recepcionar dados pessoais transferido da UE. A intenção de obter esse reconhecimento já foi evidenciada pela Corte Constitucional colombiana na Sentença C-748, de 2011, ao destacar que, por meio da implementação da Lei nº 1.581/2012, busca-se não apenas fornecer a proteção de dados nos termos exigidos pela Constituição, mas também garantir que o país cumpra os padrões internacionais na matéria para alcançar as certificações necessárias e se inserir no mercado como um território com nível adequado de proteção. Em 2019, a SIC e a Comissão Europeia iniciaram conversas preliminares sobre a avaliação da adequação da Colômbia.[381]

A despeito disso, ao fazer parte dos Estados-membros da OCDE, a Colômbia se destaca no cenário internacional de proteção de dados.[382] Além disso, com a adesão à Convenção de Budapeste, em 2020, e a assinatura do Segundo Protocolo Adicional, em 2022, a Colômbia passou a integrar a rede internacional de cooperação e combate a crimes cibernéticos. No cenário latino-americano, a Colômbia é reconhecia pela sua atuação ativa na RIPD. A SIC foi responsável pela Presidência da RIPD, durante o biênio 2021-2022. As funções da Presidência incluem representar a RIPD nos fóruns nacionais e internacionais voltados para a proteção de dados, incentivar e apoiar iniciativas legislativas relacionadas ao tema e presidir a sessões do Comitê Executivo. Atualmente, a Colômbia integra o Comitê Executivo da RIPD. [383]

2.3.4. Brasil

A Constituição brasileira de 1988 reconhece, por meio do artigo 5º, os direitos fundamentais à intimidade, à vida privada e à proteção dos dados pessoais. Além disso, esse dispositivo determina a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e telefônicas. Ainda, estabelece o *Habeas Data*

---

[381] BELLI, et. al. Hacia un modelo latino-americano de adecuación para la transferência internacional de datos personales. **Discussion paper presentado en la Computers, Privacy and Data Protection Conference Latin America (CPDP LatAm).** 2023. p. 27. Disponível em: https://cpdp. lat/wp-content/uploads/2023/07/doc-discusion-cpdplatam23-2.3.pdf. Acesso em: 2 nov. 2023.

[382] OCDE. **Colombia's path towards OECD accession**. 15 jan. 2020. Disponível em: https://www.oecd.org/colombia/colombia-accession-to-the-oecd.htm. Acesso em: 2 nov. 2023.

[383] REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. **Órganos de la Red Iberoamericana de Protección de Datos**. 2023. Disponível em: https://www.redipd.org/es/la-red/organos-de-la-red-iberoamericana-de-proteccion-de-datos. Acesso em: 2 nov. 2023.

como ação processual para conhecer, acessar e retificar informações pessoais. Diferentemente de outros países latino-americanos, no Brasil, esse instrumento se restringe às informações e dados constantes em registros ou bancos de dados de natureza pública. Confira-se a redação dos referidos artigos constitucionais:[384]

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X –são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;
> LXXII – conceder-se-á "habeas-data": a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;
> LXXIX – é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

O direito fundamental à proteção de dados pessoais recebeu significativo reconhecimento no Brasil, encontrando expressão na Constituição. No entanto, deve-se notar que esse direito apenas foi incorporado ao texto da Constituição recentemente. A trajetória até o reconhecimento de um direito constitucional autônomo à proteção de dados é marcada por avanços jurisprudenciais e desenvolvimentos legais. O entendimento originário que predominou no direito brasileiro era de que apenas a comunicação dos dados seria protegida pela Constituição, não os dados em si.[385] Essa interpretação, foi acolhida em decisões do Supremo Tribunal Federal (STF).[386] Sob essa perspectiva, o foco principal era a proteção das comunicações contra a interceptação de terceiros, a menos que houvesse uma base legal e uma ordem judicial para tal intervenção, nos termos do artigo 5º, inciso XII, da Constituição.

Segundo Laura Schertel Mendes,[387] uma mudança relevante na interpretação constitucional brasileira ocorreu em 2017 com o julgamento do Recurso Extraordinário

---

[384] BRASIL. Constituição. **Constituição da República Federativa do Brasil**, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 2 nov. 2023.

[385] FERRAZ JUNIOR, Tercio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista Tributária e de Finanças Públicas**, São Paulo, v. 1, out. 1992.

[386] BRASIL. Supremo Tribunal Federal. **RE 418.416-8, Relator Min. Sepúlveda Pertence, Dj. 10.5.2006; HC 91.867, Relator Min. Gilmar Mendes, Dj. 24.4.2012**.

[387] MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados de uma mesma moeda. **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 12, n. 39, 2018. pp. 185-216.

nº 673.707 pelo STF.[388] O caso envolvia a recusa de um pedido de acesso a informações do Sistema de Conta Corrente da Receita Federal do Brasil, feito por meio da ação de *Habeas Data*. Em sede de recurso, o STF reconheceu que as informações pessoais mantidas pela entidade, por serem capazes de identificar o indivíduo, podem afetar os seus direitos e, consequentemente, requerem proteção constitucional por meio do *Habeas Data*.[389] Para a autora, a decisão foi determinante na jurisprudência constitucional brasileira e possibilitou o uso mais amplo do *Habeas Data*.[390]

Ao contrário da experiência de outros países latino-americanos, no Brasil, a garantia do *Habeas Data* teve pouca repercussão nas práticas dos tribunais. A doutrina atribui esse diagnóstico à forma pela qual o instituto foi concebido e efetivado no ordenamento jurídico brasileiro.[391] O *Habeas Data* foi idealizado pelo constituinte de 1988 como um instrumento de passagem do regime ditatorial para a democratização, limitando-se a uma ação constitucional.[392] Seu rito processual é regulamentado pela Lei nº 9.507, de 1997, mas não foi dada a amplitude necessária para enfrentar diretamente problemas de proteção de dados.[393] Contrapondo-se a essas limitações, ao julgar o RE nº 673.707, o STF consolidou um importante passo na interpretação da proteção de dados pessoais como um direito fundamental.[394]

A elevação do status da proteção de dados a um direito constitucional autônomo ocorreu efetivamente em 2020, no julgamento, pelo STF, das Medidas Cautelares nas Ações Diretas de Inconstitucionalidade nº 6.387, 6.388, 6.389, 6.390 e 6.393, contra a Medida Provisória nº 954/2020[395], que impunha às operadoras de telefonia o compartilhamento de dados pessoais de seus usuários com o Instituto Brasileiro de Geografia e Estatística (IBGE).[396] No caso, a Medida Provisória atribuía finalidade

---

[388] BRASIL. Supremo Tribunal Federal. **RE 673.707, Relator Min. Luiz Fux, Dj. 17.6.2017.**
[389] MENDES, 2018. pp. 195-197.
[390] MENDES, 2018 p. 198.
[391] DONEDA, 2008. p. 27.
[392] DONEDA, 2008. pp. 27-28.
[393] BRASIL. Lei nº 9.507/1997, de 12 de novembro de 1997. **Regula o direito de acesso a informações e disciplina o rito processual do habeas data**. Diário Oficial da União - Seção 1 - 13/11/1997, Página 26025.. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9507.htm. Acesso em: 2 nov. 2023.
[394] MENDES, 2018. p. 198.
[395] BRASIL. Medida Provisória Nº 954/2020. **Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 2 nov. 2023.
[396] BRASIL. Supremo Tribunal Federal. **ADIs 6.387, 6.388, 6.389, 6.390 e 6.393, Relatora Rosa Weber, Dj. 7.5.2020**.

diversa, por parte do IBGE, ao tratamento de dados pessoais originalmente obtidos no âmbito de uma relação de consumo. [397] A essa altura, o Brasil já havia sancionado uma lei destinada à proteção de dados pessoais, porém as suas disposições ainda não eram aplicáveis devido ao período de *vacatio legis*, conforme será analisado adiante.

Ao apreciar a matéria, o STF reconheceu que o direito à proteção dos dados surge da necessidade de reinterpretar a Constituição brasileira frente aos avanços tecnológicos e aos impactos do tratamento à esfera de garantias fundamentais dos indivíduos, como a liberdade individual, a privacidade e o livre desenvolvimento da personalidade. Dentre os fundamentos da decisão, foi identificado que não existem dados neutros ou insignificantes. Qualquer dado que possa identificar um indivíduo pode ser valiosa tanto para o mercado quanto para o Estado, justificando assim sua tutela constitucional.[398]

Tal como já sustentando pela doutrina brasileira, não seria possível proporcionar uma tutela efetiva aos dados pessoais na amplitude que a importância do tema merece apenas sob o paradigma da interceptação das comunicações.[399] Na esteira da jurisprudência do STF, em 2022, foi aprovada a Emenda Constitucional nº 115, que, posteriormente, incorporou textualmente o direito à proteção de dados ao rol de direitos fundamentais da Constituição brasileira.[400]

2.3.4.1. A Lei Geral de Proteção de Dados brasileira

Além das garantias constitucionais, o uso de dados pessoais no Brasil foi disciplinado ao longo do tempo por leis setoriais, cuja natureza envolve o direito público e o privado.[401] Na década de 1990, o Código de Defesa do Consumidor introduziu disposições específicas sobre a abertura de bancos de dados de consumidores e de

---

[397] BIONI, Bruno; ZANATTA, Rafael A.; RIELLI, Mariana. Caso: IBGE vs. CFOAB e outros (ADIs 6.387, 6.388, 6.389, 6.390 e 6.393). **Revista de Direito Civil Contemporâneo**, vol. 26, 2021, pp. 363-391.

[398] MENDES, Laura Schertel; DA FONSECA, Gabriel Campos Soares. STF reconhece direito fundamental à proteção de dados. **Revista de Direito do Consumidor**, vol. 130, 2020.

[399] DONEDA, 2011. p. 106.

[400] BRASIL. Emenda Constitucional nº 115/2022: **altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais**. 10 fev. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20Nº%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais. Acesso em: 2 nov. 2023.

[401] VERONESE, Alexandre; MELO, Noemy. A proposta brasileira de proteção de dados pessoais e comparação ao novo regulamento europeu. **Revista de Direito Civil Contemporâneo**, vol. 14, 2018.

cadastros de inadimplentes.[402] Com as evoluções tecnológicas, a Lei do Cadastro Positivo, aprovada em 2011, estabeleceu regras objetivas para a criação de bancos de dados que reúnem informações sobre bons pagadores para a formação de histórico de crédito.[403] Em 2019, a Lei do Cadastro Positivo foi alterada para determinar a inclusão automática de indivíduos aos bancos de dados no âmbito desse sistema, com a possibilidade de solicitar a sua exclusão.[404] A Lei de Acesso à Informação, sancionada em 2011, determinou condições mínimas de acesso a dados pessoais para as entidades sujeitas à norma.[405] Ainda, o Marco Civil da Internet, aprovado em 2014, regulou o tratamento de dados coletados por meio da internet.[406]

Apesar de regramentos esparsos que tangenciam a proteção de dados, o ordenamento jurídico brasileiro carecia de uma legislação abrangente destinada ao tema. Essa lacuna distanciava o Brasil dos padrões internacionais de proteção de dados, que já haviam sido adotadas por outros países da América Latina. A urgência em estabelecer uma normativa de proteção de dados na região foi discutida no contexto do Mercosul e, em meados de 2005, a Argentina propôs um documento que, embora não tenha sido referendado pelo bloco, mais tarde serviu como inspiração para o anteprojeto de lei brasileiro.[407-408]

---

402 BRASIL. Lei nº 8.078/1990. **Dispõe sobre a proteção do consumidor e dá outras providências**. 11 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 2 nov. 2023.

403 BRASIL. Lei nº 12.414/2011. **Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito**. 9 jun. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 2 nov. 2023.

404 BRASIL. Lei Complementar nº 166/ 2019**. Altera a Lei Complementar nº 105, de 10 de janeiro de 2001, e a Lei nº 12.414, de 9 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores**. 8 abr. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp166.htm. Acesso em: 2 nov. 2023.

405 BRASIL. Lei nº 12.527/2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências**. 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 2 nov. 2023.

406 BRASIL. Lei nº 12.965/2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. 23 abr. 2014 Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 2 nov. 2023.

407 VIOLA, Mario; FRANCA, Marcílio; DONEDA, Danilo. **Festa para a proteção de dados na América do Sul**. ConJur, 17 fev. 2021. Disponível em: https://www.conjur.com.br/2021-fev-17/opiniao-festa-protecao-dados-america-sul. Acesso em: 2 nov. 2023

408 MERCOSUL. **XII Reunion ordinaria del subgrupo de trabajo n. 13 – Comercio Electronico**, 2004. Disponível em: https://documentos.mercosur.int/simfiles/docreuniones/23116_SGT13_2004_ACTA02_ES.pdf. Acesso em: 2 nov. 2023.

Como resultado de um processo legislativo que durou, no mínimo, oito anos, caracterizado por intensos debates multissetoriais no Congresso Nacional do Brasil, a Lei nº 13.709, conhecida como Lei Geral de Proteção de Dados (LGPD), foi sancionada em 2018 e entrou em vigor em setembro de 2020.[409] Alinhada ao RGPD, a LGPD estabeleceu princípios gerais, direitos para os titulares dos dados, deveres para os agentes envolvidos em atividades de tratamento, tanto público quanto privados, além de ter como um de seus pilares a criação de uma autoridade administrativa para supervisão.[410] A LGPD alocou um capítulo exclusivo para abordar as transferências internacionais de dados pessoais, conforme será analisado no Capítulo 3. Apesar do desenvolvimento tardio, quando comparado aos demais países latino-americanos abordados, com a implementação da LGPD, o Brasil se alinha aos países que possuem leis gerais de proteção de dados.

Contudo, conforme analisado na Seção 2.1.3, a proteção integral de dados pessoais requer o estabelecimento de balizas para a tutela do tratamento de dados pessoais em contextos diversos. No Brasil, nota-se a discussão para instituir lei específica sobre a proteção de dados na segurança pública e na persecução penal, semelhante ao modelo europeu que tem o RGPD e a LED. [411] Para preencher essa lacuna, uma comissão de juristas propôs o anteprojeto conhecido como "LGPD Penal".[412] Apesar de a proteção de dados ser reconhecida como um direito constitucional no Brasil, a inexistência de uma lei específica no país para proteger os dados pessoais tratados na esfera criminal e de segurança pública pode acarretar insegurança jurídica, afetando a capacidade de condução de investigações e a garantia dos direitos dos titulares dos dados.[413] O mesmo ocorre no caso da segurança e defesa nacional. Na Argentina, no Uruguai e na Colômbia, não se observou debate similar com a mesma intensidade.

---

[409] MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, v. 120, 2018. p. 555.

[410] MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, 2020. p. 15.

[411] VIOLA, Mario et al. **O anteprojeto da LGPD Penal e as regras sobre transferência internacional de dados pessoais**. Instituto de Tecnologia & Sociedade do Rio em parceria com a Embaixada Britânica no Brasil. Ago. 2021. p. 28. Disponível em: https://itsrio.org/pt/publicacoes/o-anteprojeto-da-lgpd-penal-e-as-regras-sobre-transferencia-internacional-de-dados-pessoais/. Acesso em: 2 nov. 2023.

[412] CORDEIRO, Nefi et alli. **Anteprojeto de Lei de proteção de dados para segurança pública e persecução penal. Brasília:** Poder 360, 2020. Disponível em: https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf. Acesso em: 2 nov. 2023.

[413] VERONESE, Alexandre; CALABRICH, Bruno. Crimes na internet e o Brasil no cenário de cooperação jurídica internacional: **a convenção de Budapeste e o Cloud Act dos Estados Unidos**. JOTA, 24 abr. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/judiciario-e-sociedade/crimes-na-internet-e-o-brasil-no-cenario-de-cooperacao-juridica-internacional-24042021. Acesso em: 2 nov. 2023.

2.3.4.2. A Autoridade de Proteção de Dados Pessoais brasileira

A Autoridade Nacional de Dados Pessoais (ANPD) é o órgão estabelecido pelo artigo 55-A da LGPD. Desde a sua concepção, o regime jurídico que define a estrutura da ANPD sofreu várias modificações. O projeto de lei que resultou na LGPD determinava que a ANPD tivesse um regime autárquico especial, similar ao das agências reguladoras no país, mas esse dispositivo foi vetado pelo Presidente da República. Após duras críticas, a Lei nº 13.853/2019[414] reintroduziu a ANPD na LGPD, definindo-a como um órgão subordinado à Presidência, com natureza transitória. Por fim, a Medida Provisória nº 1.124/2022, convertida na Lei nº 11460/2022, consolidou essa transição, transformando a ANPD em uma autarquia especial dotada de autonomia técnica e decisória.[415]

Compete à ANPD, entre outras funções, zelar pela proteção de dados no país, emitir regulamentos, fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à LGPD. Ainda, a ANPD tem poderes para promover ações de cooperação com APD de outros países de natureza internacional ou transnacional. No âmbito da sua atividade normativa, em 2023, a ANPD divulgou a proposta de regulamento para as transferências internacionais de dados pessoais (Regulamento de TIDP), que será examinada no Capítulo 3.[416] O documento foi submetido à consulta pública e à audiência pública, de modo a viabilizar a participação da sociedade civil e ainda poderá estar sujeito a mudanças.[417]

2.3.4.3. O Brasil nos cenários internacional e regional

Assim como a Colômbia, o Brasil não conta com uma decisão de adequação da Comissão Europeia para recepcionar dados pessoais transferido da UE. No entanto, o Brasil tem feito esforços para aumentar sua visibilidade em nível internacional no cenário

---

[414] BRASIL. Lei nº 13.853/ 2019. **Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências**. 8 jul. 2019 Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 5 nov. 2023.

[415] MAFFINI, Rafael; CARVALHO, Luciana Luso de. A atribuição do regime autárquico especial à Autoridade Nacional de Proteção de Dados. **Revista de Direito do Consumidor**, v. 144, 2022.

[416] ANPD. **Regulamento de Transferências Internacionais de Dados Pessoais.** 2023. Disponível em: https://www.gov.br/participamaisbrasil/regulamento-de-transferencias-internacionais-de-dados-pessoais-e-do-modelo-de-clausulas-padrao-contratuais. Acesso em: 2 nov. 2023.

[417] ANPD. **Aberta Consulta Pública sobre norma de transferências internacionais de dados pessoais**. 15 ago. 2023(b). Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/aberta-consulta-publica-sobre-norma-de-transferencias-internacionais-de-dados-pessoais. Acesso em: 2 nov. 2023.

de proteção de dados. Ainda que não seja signatário da Convenção da 108 e da 108+ do Conselho da Europa, em 2022 e em 2023, o Brasil, representado pelos membros da ANPD, participou das reuniões plenárias do Comitê Consultivo da Convenção, que trataram de instrumentos contratuais no contexto das transferências internacionais de dados pessoais.[418-419] Outro ponto de destaque foi a ratificação do Brasil à Convenção de Budapeste em 2022.[420] No contexto latino-americano, a ANPD tornou-se membro efetivo da RIPD, em 2021.[421] O Brasil também está envolvido nas ações da Agenda Digital do Mercosul. [422]

2.4. Conclusão do Capítulo

Com base nas distintas construções jurídicas em matéria de proteção de dados da UE e dos EUA analisadas neste Capítulo, enquanto a UE desenvolveu um sistema jurídico robusto, cujo quadro legal hoje inclui o RGPD e a LED, e permite a postulação de direitos substantivos perante as APD, os EUA contam com uma estrutura fragmentada que combina leis setoriais, tanto no âmbito federal quanto estadual, regulamentos e autorregulação. No entanto, a abordagem norte-americana parece estar destinada a mudanças, aproximando-se dos padrões regulatórios de proteção de dados da UE. A Ordem Executiva do Presidente Biden sobre o Desenvolvimento, Uso Seguro, Protegido e Confiável de Inteligência Artificial, que sinaliza ao Congresso que avance com a aprovação de uma legislação federal bipartidária de privacidade, é um passo nessa direção.

A análise sobre os modelos regulatórios da UE e dos EUA demonstra que a interconexão entre os diferentes sistemas jurídicos de proteção de dados é essencial para as transferências internacionais de dados pessoais. Como evidenciado neste Capítulo, o processo de avaliação de adequação conduzida pela Comissão Europeia para autorizar as

---

[418] ANPD. **ANPD participa da 43ª Reunião Plenária da Convenção 108, na França**. 17 nov. 2022. Disponível em:https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-participa-da-43a-reuniao-plenaria-da-convencao-108-na-franca. Acesso em: 2 nov. 2023.

[419] ANPD. **ANPD representa o Brasil na 44ª Reunião Plenária do Comitê Consultivo da Convenção 108**. 15 jun. 2023(c). Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-representa-o-brasil-na-44a-reuniao-plenaria-do-comite-consultivo-da-convencao-108. Acesso em: 2 nov. 2023.

[420] BRASIL**.** Ministério da Justiça e Segurança Pública**. Convenção de Budapeste é promulgada no Brasil,** 17 abr. 2023. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso em: 2 nov. 2023.

[421] ANPD. **ANPD torna-se membro da Rede Ibero-Americana de proteção de dados**. 21 out. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-torna-se-membro-da-rede-ibero-americana-de-protecao-de-dados Acesso em: 2 nov. 2023.

[422] MERCOSUL. **Agenda Digital**. 2023. Disponível em: https://www.mercosur.int/pt-br/temas/agenda-digital/. Acesso em: 2 nov. 2023.

transferências de dados para países terceiros pode não acompanhar o aumento dos fluxos de dados. Por sua vez, as salvaguardas previstas no RGPD baseadas em cláusulas contratuais padrão, normas corporativas vinculantes, códigos de conduta e certificações, juntamente com a supervisão das APD, são instrumentos híbridos e representam meios para promover as transferências. Sob a LED, as salvaguardas se diferenciam daquelas previstas no RGPD, demandando supervisão ainda mais acentuada das APD para a tutela dos dados pessoais nas transferências.

Os desafios para o fluxo de dados entre UE e EUA motivaram trabalhos conjuntos para que fossem desenvolvidos arranjos intermediárias que pudessem otimizar as transferências de dados pessoais entre as regiões. Contudo, as tensões marcadas pela invalidação do *Safe Harbor* e do *Privacy Shield* pela TJUE e pela recente decisão do IDPC sublinharam um problema reiterado que se traduz na dependência do setor público no acesso a dados pessoais obtidos pelo setor privado para desempenhar atividades de segurança. Nesse particular, após a decisão do caso Schrems II pelo TJUE, os agentes que adotarem cláusulas contratuais padrão para realizar as transferências também devem incorporar avaliações de risco para determinar se as normas do país terceiro admitem a divulgação de dados para autoridades públicas. Essa discussão ressalta a necessidade de que sejam estabelecidas balizas para a proteção integral de dados, abrangendo contextos diversos que envolvem atividades de segurança e a investigação e repressão criminal.

Com a vigência do novo *Data Privacy Framework* e, sobretudo com as salvaguardas decorrentes da Ordem Executiva do Presidente Biden sobre o Fortalecimento das Proteções das Atividades de Inteligência de Sinais, o futuro das transferências de dados pessoais entre UE e EUA vai depender da efetividade dos mecanismos institucionais dos EUA, em especial a atuação do Oficial de Proteção às Liberdades Civis e da Corte de Revisão de Proteção de Dados. A Ordem Executiva igualmente poderá acarretar impactos para além da relação UE-EUA, tendo em vista, entre outros aspectos, a designação pelo Procurador-Geral dos EUA de países considerados "Estados qualificados", nos quais os indivíduos também poderão dispor dos mecanismos institucionais estabelecidos nos EUA.

Na América Latina, a evolução da proteção de dados traz repercussões da modelagem da UE e dos EUA e possui particularidades atreladas a razões históricas, econômicas, políticas e sociais, além de uma demanda global crescente contemplada na adesão a instrumentos internacionais e regionais. Nesse cenário, o *Habeas Data* emergiu como um fenômeno típico da região, variando em relação à sua abrangência e eficácia, a

depender do país. À medida que aspectos regulatórios para a proteção de dados avançavam nos países latino-americanos, alguns deles pareciam seguir o modelo norte-americano, especialmente devido à importância dada à interpretação judicial pela ação de *Habeas Data*. No entanto, com o tempo, percebeu-se a expansão do modelo regulatório europeu na região, evidenciando o reconhecimento do direito à proteção de dados como um direito fundamental. A difusão dos padrões da UE para proteção de dados pessoais permitiu o maior engajamento dos países latino-americanos nesse debate, o que reflete também a evolução global do tema.

No decorrer das duas últimas décadas, o Brasil, a Argentina, o Uruguai e a Colômbia desenvolveram modelos jurídicos de proteção de dados, incorporando preceitos e instrumentos processuais nas suas constituições nacionais, que revelam o compromisso de garantir a proteção contra o uso inadequado de dados pessoais. Além disso, tais países aprovaram leis gerais de proteção de dados e instituíram autoridades administrativas com poderes para aplicar e supervisionar as suas disposições legais. Observa-se também um crescente movimento de adesão dos países latino-americanos a instrumentos internacionais, como a Convenção 108 e 108+ e a Convenção de Budapeste do Conselho da Europa. Paralelamente, nota-se um fortalecimento regional significativo do tema com a atuação da RIDP, incluindo esforços para o intercâmbio de informações entre as APD.

No entanto, como evidenciado no conflito transatlântico entre UE e EUA, há uma agenda de proteção aos dados pessoais referente às atividades de segurança persecução penal que requer atenção. Ela, inclusive, é capaz de influenciar a avaliação e a própria revisão do nível de proteção de um país no âmbito de fluxos comerciais e civis, como ocorreu com as decisões do TJUE, nos casos Schrems I e II, e a decisão do IDPC analisadas. Nesse sentido, uma questão que deve ser considerada pelos países latino-americanos abordados é como seus respectivos quadros legais de proteção de dados pessoais poderão ser aprimorados para cobrir essa agenda frente aos desafios atuais, com o intuito de garantir transferências internacionais de dados pessoais seguros e confiáveis.

Com base na análise deste Capítulo, o Quadro 1, abaixo, resume as principais disposições constitucionais, as leis gerais de proteção de dados, os regulamentos vigentes e as autoridades estabelecidas em cada país analisado, e foi elaborado para servir de referência para a investigação dos regimes de tutela das transferências internacionais de dados pessoais do Brasil, da Argentina, do Uruguai e da Colômbia.

Quadro 1 – Quadro constitucional e legal de proteção de dados do Brasil, da Argentina, do Uruguai e da Colômbia.

País	Constituição	Legislação geral de proteção de dados e principais regulamentos	Autoridade de Proteção de Dados
Argentina	Artigos 18, 19 e 43	• Lei nº 25.326/2000 • Decreto nº 1558/2001	AAIP/DNPDP
Uruguai	Artigos 10, 28, 72 e 332	• Lei nº 18.331/2008 • Decreto n° 414/2009 • Lei 19.670/2018 • Decreto nº 64/2020	URCDP
Colômbia	Artigos 15 e 20	• Lei nº 1.581/2012 • Decreto nº 1377/ 2013	SIC
Brasil	Artigos 5º, XV, XII, LXXII e LXXIX	• Lei nº 13.709/2018 (LGPD)	ANPD

Fonte: elaboração própria.

À luz do panorama jurídico acima descrito, o Capítulo seguinte passa a analisar as transferências internacionais de dados pessoais em perspectiva comparada.

3. TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PESSOAIS EM PERSPECTIVA COMPARADA

3.1. A delimitação do conceito jurídico de transferência internacional de dados pessoais

Antes de tratar dos regimes de tutela das transferências internacionais de dados propriamente ditos, é necessário delimitar o conceito jurídico que qualifica tal transferência nos países abordados. Examinemos, portanto, as definições relevantes para a caracterização das transferências internacionais de dados pessoais, conforme estabelecido pelos marcos jurídicos de proteção de dados da Argentina, doUruguai, da Colômbia e do Brasil.

Em linhas gerais, as legislações de proteção de dados abarcadas neste estudo definem os agentes envolvidos no tratamento de dados, sejam eles de natureza pública ou privada, como o controlador (em espanhol, *responsable del tratamiento*)[423] e o operador (em espanhol, *encargado del tratamiento*).[424] Com relação às atribuições de tais agentes, o controlador é aquele que assume as decisões referentes ao tratamento de dados. Em alguns casos, o controlador está relacionado com a titularidade de bancos e bases de dados, como na Argentina e no Uruguai. O operador, por sua vez, é o agente que realiza o tratamento de dados pessoais em nome do controlador. Diferentemente dos demais países analisados, embora a lei argentina não estabeleça expressamente o conceito de operador, tal figura é delineada no contexto de prestação de serviços, situação em que o

[423] Respectivamente, as definições de controlados nas leis de proteção de dados da Argentina, Uruguai, Colômbia e Brasil:
Lei nº 25.326/2000. Art. 2º: *Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.*
Lei nº 18.331/2008. Art. 4, "k": *Responsable de la base de datos o del tratamiento: persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento.*
Lei nº 1.581/2012. Art. 3º, "e": *Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.*
LGPD. Art. 5º, VI: Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

[424] Respectivamente, as definições de operador nas leis de proteção de dados do Uruguai, Colômbia e Brasil:
Lei nº 18.331/2008. Art. 4, "h": *Encargado del tratamiento: persona física o jurídica, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable de la base de datos o del tratamiento.*
Lei nº 1.581/2012. Art. 3º, "d": *Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.*
LGPD. Art. 5º, VII: Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

operador deve realizar o tratamento sob as instruções do controlador.[425-426] Diante dessa lacuna na legislação argentina vigente, a criação do conceito de operador foi particularmente destacada no Projeto de Lei da AAIP.

Além disso, as legislações de proteção de dados dos países abordados dispõem sobre o compartilhamento de dados entre os diferentes agentes. A Lei nº 25.326/2000 da Argentina, em conjunto com o Decreto nº 1558/2001, estabelecem os conceitos de cessão de dados, prestação de serviços e transferência internacional de dados. [427] A cessão ocorre quando os dados são transferidos entre um cedente e um cessionário, dando a esse último a capacidade de tratá-los conforme seu próprio interesse.[428] A prestação de serviços envolve o envio de dados de um controlador para um operador, de acordo com as finalidades e instruções contratualmente especificadas e com a obrigatoriedade de adotar medidas de segurança.[429] A transferência internacional refere-se ao envio de dados da Argentina para outro país, incluindo no âmbito de cessão e de prestação de serviços.[430]

Similar à legislação argentina, a Lei nº 18.331/2008, do Uruguai e o Decreto n° 414/2009 definem os termos de cessão, comunicação e transferência internacional de dados.[431] A cessão e a comunicação constituem a revelação ou envio de dados a uma entidade distinta do titular, conforme as hipóteses previstas na lei uruguaia, para cumprir com as finalidades diretamente relacionadas aos interesses do remetente e do destinatário

---

[425] Decreto nº 1558/200. Art. 25: *Los contratos de prestación de servicios de tratamiento de datos personales deberán contener los niveles de seguridad previstos en la Ley Nº 25.326, esta reglamentación y las normas complementarias que dicte la Direccion Nacional De Proteccion De Datos Personales, como así también las obligaciones que surgen para los locatarios en orden a la confidencialidad y reserva que deben mantener sobre la información obtenida. La realización de tratamientos por encargo deberá estar regulada por un contrato que vincule al encargado del tratamiento con el responsable o usuario del tratamiento y que disponga, en particular: a) que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento; b) que las obligaciones del artículo 9º de la Ley Nº 25.326 incumben también al encargado del tratamiento.*

[426] FRENE, Lisandro. **El "encargado de tratamiento" de datos personales en el derecho argentino**. 14 mar. 2022. Disponível em: https://abogados.com.ar/el-encargado-de-tratamiento-de-datos-personales-en-el-derecho-argentino/30096. Acesso em: 2 nov. 2023.

[427] GONZÁLEZ ALLONCA, Juan C.; RUIZ MARTÍNEZ, Esteban. **Cloud Computing: la regulación de la transferencia internacional de datos personales y la prestación de servicios por parte de terceros. Sistema Argentino de Información Jurídica – Ministerio de Justicia y Derechos Humanos**. 1 out. 2015. Disponível em: http://www.saij.gob.ar/. Acesso em: 2 nov. 2023.

[428] Artigo 11, Lei nº 25.326/2000.

[429] Artigo 25, Lei nº 25.326/2000.

[430] Artigo 12, Lei nº 25.326/2000.

[431] AAIP; URCDP. **Guía de Evaluación de Impacto en la Protección de Datos**. 28 jan. 2020. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-evaluacion-impacto-proteccion-datos . Acesso em: 2 nov. 2023.

dos dados.[432] A transferência internacional diz respeito à cessão ou comunicação de dados que tem como destinatário uma entidade localizada fora do território uruguaio.[433]

A Lei nº 1.581/2012 da Colômbia, juntamente com o Decreto nº 1377/ 2013, estabelecem que a transferência se refere ao envio de dados pessoais de um controlador para outro. Essa transferência pode ser compreendida como a entrega de dados pessoais a uma entidade distinta do operador e do próprio titular. Ainda, a transferência de dados pode ser nacional ou internacional, ocasião em que os dados transpõem as fronteiras colombianas, sendo enviados para um destinatário localizado em país terceiro.[434] Além disso, a legislação colombiana postula que a transmissão consiste na comunicação de dados pessoais dentro ou fora do território colombiano quando tem por objetivo a realização de um tratamento pelo operador em nome de um controlador.[435] Na transmissão, o tratamento continua sob a responsabilidade do controlador que, diante de questões práticas ou de necessidade, entrega os dados ao operador para que realize o tratamento seguindo suas instruções.[436]

No Brasil, a LGPD prevê conceito amplo denominado de uso compartilhado de dados, que abrange uma variedade de atividades como comunicação, difusão, transferência internacional, interconexão de dados pessoais e tratamento compartilhado de bancos de dados pessoais, que podem ocorrer entre entidades públicas ou privadas.[437] Mais especificamente, a LGPD refere-se à transferência internacional de dados pessoais como a transferência para país estrangeiro ou organismo internacional do qual o país seja membro.[438] A proposta de regulamento de transferências internacionais de dados pessoais emitida pela ANPD reconhece que a transferência requer uma operação de tratamento por meio da qual o controlador ou operador de dados transmite, compartilha ou disponibiliza acesso aos dados pessoais a outro agente.[439]

A despeito da pluralidade terminológica adotada por cada país para tratar das diversas formas de compartilhamento de dados pessoais, ao analisar o conceito jurídico de transferências internacional de dados nas legislações latino-americanas abordadas, identifica-se uma convergência na sua definição. As transferências internacionais se

[432] Artigo 4º, "b", Lei nº 18.331/2008; Artigo 4º, "c", e artigo 14 do Decreto n° 414/009.
[433] Artigo 4º, "h", Decreto n° 414/009.
[434] Artigo 3º, item 4, Decreto nº 1377/ 2013.
[435] Artigo 3º, item 5, Decreto nº 1377/ 2013.
[436] REMOLINA, 2015. pp. 226-227.
[437] Artigo 5º, XVI, LGPD.
[438] Artigo 5º, XV, LGPD.
[439] Artigo 3º, III, da proposta de regulamento de TIDP da ANPD.

qualificam, essencialmente, pelo envio de dados pessoais de um agente para outro situado em país estrangeiro. Esta operação pressupõe dois aspectos fundamentais. Primeiro, os dados pessoais ultrapassam as fronteiras nacionais e ingressem no território do país destinatário. Segundo, os dados pessoais são remetidos entre dois ou mais agentes, que se diferem do titular dos dados.

Com base nas legislações de proteção de dados em questão, pode-se definir uma transferência internacional quando um agente, o exportador, envia dados pessoais de um país para outro agente, o importador, que está localizado em um país distinto.

3.2. A dimensão extraterritorial do direito à proteção de dados pessoais

A compreensão adequada do conceito jurídico de transferência internacional de dados igualmente requer a sua distinção de outro fenômeno que possibilita o tratamento de dados pessoais fora do país de origem, qual seja, a coleta internacional de dados. De forma geral, as legislações de proteção de dados dos países latino-americanos sob análise qualificam a coleta como uma das atividades compreendidas no tratamento de dados pessoais.[440]

Por ser o ponto de partida para as atividades de tratamento subsequentes, as leis atribuem significativa importância à legitimidade das práticas de obtenção de dados pessoais, que devem estar respaldada pelos seus princípios e requisitos. Esse cenário é ainda mais relevante diante da crescente proporção de indivíduos conectados à Internet. Conforme analisado na Seção 1.1, a Internet, em muitos casos, constitui uma ferramenta

[440] Respectivamente, as definições de tratamento de dados nas leis de proteção de dados da Argentina, Uruguai, Colômbia e Brasil:
Lei nº 25.326/2000. Art. 2º: *Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.*
Decreto nº 414 de 2009. Art. 2º: *Ambito objetivo. El régimen jurídico de la protección de datos personales se aplica a su recolección, registro y todo tipo de tratamiento, automatizado o no, bajo cualquier soporte y modalidad de uso, tanto sea en el ámbito público como privado (...).* Art. 4º, "m," da Lei nº 18.331/2008: *Tratamiento de datos: operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permitan el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias*.
Lei nº 1.581/2012. Art. 3º, "g": *Tratamiento**:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.*
LGPD. Art. 5º, X: Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

por meio da qual os próprios titulares podem fornecer os seus dados voluntariamente, o que ocorre, por exemplo, ao publicar conteúdo em mídias sociais.

Com relação à coleta internacional de dados, as leis do Brasil e da Colômbia reconhecem expressamente a natureza particular dessa atividade. No Brasil, a proposta de regulamento de transferências internacionais de dados pessoais emitida pela ANPD estabelece que a coleta internacional ocorre quando os dados pessoais são coletados diretamente por um agente localizado no exterior.[441] Na Colômbia, a Lei nº 1.581/2012 prevê que cabe à SIC solicitar a cooperação de entidades internacionais ou estrangeiras quando os direitos dos titulares forem afetados fora do território colombiano em razão de coleta internacional de dados pessoais.[442] Esse dispositivo permite que a SIC coordene ações para assegurar os direitos dos titulares e o cumprimento da lei colombiana quando há uma coleta internacional.

Nesse sentido, embora os dados saiam do país de origem, a coleta internacional de dados refere-se à obtenção direta de dados por agentes localizados fora do país no qual o titular está situado. Diferentemente da transferência internacional, essa operação não envolve a remissão de dados pessoais entre um exportador e um importador. Em vez disso, trata-se de entidade localizada em país terceiro que realiza a coleta direta dos dados, frequentemente, por meio da Internet.[443] Para alcançar situações como essas, há uma tendência nas leis gerais de proteção de dados de introduzir disposições que lhes conferem um caráter extraterritorial, como é o caso do RGPD.[444]

Na América Latina, os esforços para estender o escopo de aplicação das leis de proteção de dados foram impulsionados, em grande parte, pelo RGPD. Contudo, a edição ou atualização das leis de proteção de dados na região para compreender um alcance extraterritorial vai além do mero alinhamento com os padrões europeus. Essa iniciativa representa uma resposta ao contexto global contemporâneo, cada vez mais digitalizado e interconectado, no qual o território onde está o agente que coleta os dados é, muitas vezes, diferente do país onde está o titular.[445]

---

[441] Art. 3º, V, da proposta de regulamento de TIDP da ANPD.
[442] Art. 21, "j", Lei nº 1.581/2012.
[443] REMOLINA, 2015. p. 235.
[444] NAEF, Tobias. Data Protection Without Data Protectionism**: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law**. Springer Nature, 13 dez. 2023. p. 431.
[445] VÁSQUEZ VÉLEZ, Alejandra. **El ámbito de aplicación del régimen jurídico colombiano para la protección de datos personales. Su alcance frente a empresas extranjeras sin representación jurídica en Colombia**. Monografía jurídica para optar por el título de Abogada. Facultad de Ciencias Jurídicas Pontificia Universidad Javeriana, 2021. p. 121. Disponível em: https://repository.javeriana.edu.co/handle/10554/58083. Acesso em: 2 nov. 2023.

Nesse sentido, na Argentina, os regulamentos emitidos pela AAIP contribuíram para que a Lei nº 25.326/2000 acompanhasse os novos desafios da modernidade, ainda que a normativa tenha sido promulgada no início do novo milênio.[446] Em 2022, a AAIP disponibilizou um formulário digital para o registro de bases de dados de entidades estrangeiras que tratam dados pessoais de cidadãos argentinos, mas que não estão estabelecidos no território nacional.[447] Segundo a AAIP, o principal objetivo dessa ação é ampliar a proteção conferida aos titulares, a fim de que a ausência do agente na região não represente um impedimento para o exercício dos direitos.

A atuação da SIC na Colômbia também seguiu essa tendência. No decorrer do tempo, a SIC modificou a sua posição em relação ao âmbito de aplicação da Lei nº 1.581/2012 às empresas estrangeiras. A posição anterior sustentava que o tratamento de dados pessoais realizado por empresas no exterior por meio de redes sociais não estava sujeito à aplicação da Lei colombiana. Devido aos riscos associados ao uso inadequado de dados, a SIC revisou sua postura e passou a declarar a sua competência para fiscalizar o tratamento de dados pessoais conduzido por empresas no exterior que operam plataformas digitais que oferecem serviços para indivíduos na Colômbia, sob o fundamento de que as disposições da Lei nº 1.581/2012 são aplicáveis ao tratamento de dados pessoais no território colombiano. Desde a mudança, a SIC tem reproduzido o novo posicionamento em investigações administrativas.[448]

A ampliação do escopo de aplicação das leis de proteção de dados não se restringe à interpretação das autoridades supervisoras, mas também está contemplado nos textos legais. Como elucidado na Seção 2.3.2.3, no Uruguai, a Lei nº 18.331/2008 foi recentemente alterada pela Lei nº 19.670/2018 e pelo Decreto nº 64/2020. Um dos aspectos mais notáveis dessas modificações se reflete na expansão da aplicação da lei uruguaia para controladores e operadores localizados fora do país quando as atividades de tratamento estiverem relacionadas com a oferta de bens e serviços dirigidos a indivíduos no Uruguai, quando as normas de direito internacional público ou um contrato assim o estipularem, ou quando, no tratamento, forem utilizados meios localizados no

[446] AAIP. **Normativa**. 2023. Disponível em: https://www.argentina.gob.ar/aaip/buscador-normativa. Acesso em: 2 nov. 2023.
[447] AAIP. **Registro de Bases de Datos Personales para responsables extranjeros.** 29 nov. 2022. Disponível em: https://www.argentina.gob.ar/noticias/registro-de-bases-de-datos-personales-para-responsables-extranjeros. Acesso em: 2 nov. 2023.
[448] VÁSQUEZ, 2021. pp. 91-93.

país.[449-450] De forma similar, no Brasil, a LGPD estabelece um alcance extraterritorial ao prever que a lei brasileira se aplica a qualquer tratamento de dados, independentemente do país da sede do agente ou do país onde os dados estão localizados, desde que o tratamento seja realizado no território brasileiro, ou a atividade de tratamento tenha por objetivo a oferta de bens ou serviços ao mercado brasileiro, ou os dados tenham sido coletados no Brasil.[451]

À luz desses elementos, restam evidentes os critérios que qualificam a transferência e a coleta internacional de dados e as diferenças entre essas operações. A transferência internacional implica necessariamente no envio de dados entre dois ou mais agentes localizados em países distintos, enquanto a coleta internacional de dados é realizada diretamente por um único agente situado no exterior.[452] No contexto das transformações digitais e da crescente ubiquidade da Internet, a coleta internacional de dados frequentemente se encontra sob os efeitos extraterritoriais das leis de proteção de dados. Por sua vez, as transferências internacionais de dados pessoais estão sujeitas a regimes específicos, que serão analisados na Seção seguinte.

3.3. Os regimes de tutela das transferência internacional de dados pessoais do Brasil, da Argentina, do Uruguai e da Colômbia

Os regimes de tutela das transferências internacionais de dados, presentes nas legislações de proteção de dados do Brasil, da Argentina, do Uruguai e da Colômbia partem da premissa de que os esforços internos de proteção de dados devem manter a sua eficácia quando os dados forem transferidos para outros países. Esse entendimento é sustentado pela noção de continuidade, segundo a qual a proteção conferida aos dados deve acompanhá-los ao cruzarem as fronteiras.[453] Esta Seção objetiva aprofundar a análise de tais regimes em cada país.

Convém ressaltar, desde já, que os regimes sob análise oferecem duas principais abordagens com enfoques diferentes. A primeira, refere-se à abordagem com enfoque geográfico, que visa a garantir a proteção dos dados contra os riscos que o país destinatário dos dados possa apresentar. Essa solução compreende o processo pelo qual

[449] Artigo 37, Lei nº 19.670/2018; Artigo 1° e 2°, Decreto nº 64/2020.
[450] VÁSQUEZ, 2021. pp. 44-45.
[451] Artigo 3º, LGPD.
[452] KUNER, Christopher. Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection. **University of Cambridge Faculty of Law**, Research Paper, n. 20, 2021.
[453] NAEF, 2023. p. 155.

um país busca o reconhecimento por outro país ou por um grupo de países da existência de "nível de proteção de dados adequado" e é inspirada no requisito de adequação previsto na Diretiva 95/46/CE e, depois, no RGPD. Nesse processo, alguns países podem optar por listar os locais considerados adequados, enquanto outros podem listar os locais considerados inadequados. Além disso, há países que, em vez de construir suas próprias listas, adotam aquelas estabelecidas por outras jurisdições. Sob esse prisma, se o país destinatário possui nível adequado de proteção, a transferência internacional opera tal como uma transferência dentro das próprias fronteiras.[454]

A segunda, diz respeito à abordagem com enfoque organizacional, que requer a contenção de riscos pelos agentes que transferem os dados. Tal solução está associada à adoção de medidas pelos agentes envolvidos na transferência para assegurar a proteção dos dados transferidos.[455] Nesse caso, são utilizados mecanismos voluntários, que podem envolver, a depender do país, o estabelecimento de instrumentos contratuais entre o exportador e o importador para a transferência dos dados pessoais, a adesão a normas corporativas vinculantes ou globais ou a códigos de conduta, e a emissão de selos de garantia ou certificação correspondente de proteção de dados.[456]

Além desses dois conjuntos de abordagens, os regimes sob análise também estabelecem derrogações destinadas a cobrir situações nas quais o país para o qual os dados serão transferidos não oferece nível de proteção adequado, nem são empregados mecanismos voluntários pelo exportador e pelo importador, mas que existem outras razões que justificam a ocorrência da transferência internacional de dados pessoais.

Com base nesse panorama, a seguir, serão examinadas as abordagens e situações de derrogações descritas acima, de acordo com os regimes de tutela das transferências internacionais de dados pessoais de cada país. No final, serão analisados aspectos relevantes entre esses regimes em perspectiva comparada. Assim como no Capítulo 2, a divisão dos países nas Subseções seguintes mantém-se conforme a ordem cronológica de promulgação das leis gerais de proteção de dados.

---

[454] KUNER, 2010. pp. 27-28.

[455] KUNER, 2010. pp. 28-29.

[456] BIONI, Bruno; MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 2a ed. São Paulo: Thomson Reuters, 2020. p. 796.

3.3.1. Argentina

Na Argentina, a Lei nº 25.326/2000 juntamente com o Decreto nº 1558/2001 estabelecem três regimes que autorizam a realização de transferência internacional de dados pessoais. Primeiro, o país destinatário dos dados oferece nível de proteção adequado, de acordo com a avaliação da AAIP. Segundo, a proteção da transferência decorre de cláusulas contratuais que preveem a salvaguarda dos dados pessoais ou de sistemas de autorregulação. Terceiro, a transferência se enquadra nas exceções previstas na Lei nº 25.326/2000. Além disso, as regulamentações publicadas pela AAIP complementam as hipóteses previstas na legislação argentina.

3.3.1.1. Nível adequado de proteção de dados do país terceiro

O artigo 12 da Lei nº 25.326/2000 e o Decreto nº 1558/2001 proíbem transferências de dados pessoais de qualquer tipo com países ou organizações internacionais ou supranacionais que não ofereçam níveis de proteção adequados. Para efeitos da legislação argentina de proteção de dados, o nível será considerado adequado quando a proteção decorrer diretamente do ordenamento jurídico vigente do país terceiro ou de salvaguarda proporcionada por cláusulas contratuais que preveem a proteção de dados pessoais ou de sistemas de autorregulação.[457]

A esse respeito, o artigo 12 do Decreto nº 1558/2001 dispõe que a AAIP poderá avaliar, de ofício ou a pedido da parte interessada, o nível de proteção conferido pelas normas de um país ou organismo internacional, considerando todas as circunstâncias que ocorrem em uma transferência ou em uma categoria de transferências de dados. Em particular, será observada a natureza dos dados, a finalidade e a duração do tratamento, o local de destino, as normas, gerais ou setoriais, em vigor no país em questão, bem como as normas profissionais, códigos de conduta e medidas de segurança vigentes nesses lugares ou aplicáveis a organizações internacionais ou supranacionais. Segundo Pablo Palazzi, caso a AAIP identifique que um país não protege devidamente os dados pessoais, deverá propor um decreto ao Poder Executivo nacional para esta declaração. Embora a legislação argentina possibilite a criação de uma lista de países inadequados, essa medida nunca foi adotada na prática.[458]

---

[457] AAIP.**Obligaciones de los responsables de bases de datos personales**. 2023(b). Disponível em: https://www.argentina.gob.ar/aaip/datospersonales/responsables/obligaciones. Acesso em: 2 nov. 2023.
[458] BELLI, et. al., 2023. p. 14.

Nos termos da *Disposición* nº 60 de 2016,[459] posteriormente atualizada pela *Resolución* nº 34 de 2019 da AAIP,[460] os países considerados com nível de proteção adequado pela AAIP, até a data de conclusão desta pesquisa, são: Estados-Membros da UE e membros do Espaço Econômico Europeu, Reino Unido da Grã-Bretanha e Irlanda do Norte, Suíça, Guernsey, Jersey, Ilha de Man, Ilhas Faroé, o setor privado do Canadá, Principado de Andorra, Nova Zelândia, Uruguai e Estado de Israel (apenas com relação aos dados que recebem tratamento automatizado). Na *Disposición* nº 60/2016, ressalta-se que foi analisada a legislação dos países classificados como adequados na UE, o que levou à conclusão sobre o nível equivalente desses países com relação à Lei nº 25.326/2000. A AAIP pode, por iniciativa própria ou a pedido de partes interessadas, rever a lista de países adequados e realizar estudos sobre outros países ou organismos internacionais.

3.3.1.2. Cláusulas-padrão Contratuais

O artigo 12 do Decreto nº 1558/2001 igualmente reconhece que a transferência terá nível de proteção adequado quando tal proteção decorrer de cláusulas contratuais. De modo a determinar o conteúdo e os requisitos necessários para que as cláusulas contratuais assegurem a proteção dos dados transferidos para países que não possuem legislação adequada, a *Disposición* nº 60/2016 da AAIP aprovou dois conjuntos de cláusulas-padrão contratuais. Tais instrumentos contemplam as alternativas práticas mais comuns de transferência internacional previstas na legislação argentina, quais sejam, a cessão de dados pessoais e a prestação de serviços.[461]

Antes da *Disposición* nº 60/2016, a AAIP não exigia aprovação prévia para contratos de transferência internacional de dados e não havia um modelo padrão para as cláusulas contratuais. Mesmo sem essa exigência, a AAIP poderia analisar e opinar sobre a adequação dos contratos, a pedido de uma das partes, o que ensejou o desenvolvimento de uma jurisprudência administrativa sobre o tema. Na prática, muitos seguiam modelos próximos aos da UE, com ajustes para a legislação local.[462]

---

[459] AAIP.**Disposición nº 60/2016: Clausulas Contractuales Tipo de Transferencia Internacional - Aprobacion**. Disponível em: https://www.argentina.gob.ar/normativa/nacional/267922/texto. Acesso em: 2 nov. 2023.

[460] AAIP.**Resolución nº 34/2019: Disposicion 60 - E/2016 - Modificacion**. 22 fev. 2019 Disponível em https://www.boletinoficial.gob.ar/detalleAviso/primera/202373/20190226. Acesso em: 2 nov. 2023.

[461] AAIP. **Disposición nº 60/2016: Clausulas Contractuales Tipo de Transferencia Internacional - Aprobacion**. Disponível em: https://www.argentina.gob.ar/normativa/nacional/267922/texto. Acesso em: 2 nov. 2023.

[462] BELLI, et. al., 2023. pp. 8-9.

Para a AAIP, a aprovação das cláusulas-padrão contratuais oferece parâmetros para garantir a efetivação dos direitos dos titulares. A sua elaboração considerou a experiência internacional, especialmente no que se refere às conclusões do documento sobre transferências de dados pessoais para países terceiros do Grupo de Trabalho do Artigo 29, da Diretiva 95/46/CE e das cláusulas-padrão contratuais aprovadas pela Comissão Europeia, em 2001 e em 2010. O Plano Estratégico da AAIP 2022-2026 estabeleceu como meta a atualização das cláusulas-padrão contratuais argentinas, o que foi motivado, sobretudo, pela aprovação das novas cláusulas-padrão contratuais pela Comissão Europeia em 2021.[463]

As cláusulas-padrão contratuais da AAIP disciplinam, entre outros aspectos, o detalhamento da transferência e das finalidades pretendidas; a alocação de obrigações e responsabilidades para o exportador e o importador à luz da legislação argentina de proteção de dados; as responsabilidades e as exigências de terceiros beneficiários; a instituição da legislação e jurisdição argentinas para reger os conceitos, as cláusulas e a identificação da AAIP como autoridade; os critérios para dirimir conflitos com os titulares de dados; as condições de resolução, incluindo quando houver o descumprimento das obrigações estipuladas pelo importador e outras circunstâncias como o reconhecimento de violações por quaisquer uma das partes por meio de decisões judiciais definitivas e irrecorríveis dos tribunais argentinos ou da AAIP. Mais especificamente, no caso da prestação de serviços, o importador deverá tratar os dados conforme as instruções do exportador, além de destruir ou devolver os dados ao exportador, após o término do contrato.

Os agentes que implementarem contratos de transferência de dados que se diferem das cláusulas padrão da AAIP e que não refletem os princípios, salvaguardas e conteúdo relacionado à proteção de dados pessoais contidos nos modelos aprovados devem submetê-los à aprovação da AAIP. O procedimento para a aprovação envolve a elaboração de uma solicitação de aprovação do instrumento contratual à AAIP contendo a explicação de como o contrato apresentado se difere das cláusulas-padrão contratuais previstas na *Disposición* nº 60/2016 da AAIP, bem como a sua compatibilidade com a Lei nº 25.326/2000 e, por fim, o fornecimento de cópias do contrato.

Cabe destacar que, ainda que não se identifique previsão expressa na legislação argentina de proteção de dados para a condução de uma avaliação de impacto

[463]AAIP. Resolución 94/2023**: Plan Estrategico 2022-2026**. 23 mai. 2023(d). Disponível em: https://www.boletinoficial.gob.ar/detalleAviso/primera/287117/20230524. Acesso em: 2 nov. 2023.

a respeito da transferência internacional que se pretende realizar, essa prática é reconhecida pela AAIP no *Guia de Evaluación de Impacto en la Protección de Datos*, elaborado em conjunto com a URCDP, que será examinado adiante.[464]

3.3.1.3. Cláusulas Contratuais Modelo aprovadas pela RIPD

Recentemente, a AAIP aprovou a *Resolución* nº 198, de 2023, e passou a reconhecer as cláusulas contratuais modelo aprovadas pela RIPD, incluídas no Guia para Implementação de Cláusulas Contratuais Modelo, como mecanismos válidos para as transferências internacionais de dados pessoais a partir da Argentina.[465] A AAIP considera que, diante do crescimento significativo dos fluxos de dados para além das fronteiras e seu impacto na economia global, em níveis regional e internacional, avançou-se na atualização das cláusulas contratuais para a transferência internacional, com o propósito de conduzir à convergência de ferramentas, simplificar os procedimentos e estabelecer bases de garantias comuns que potencializem a confiança entre os diferentes países.

Para a AAIP, as cláusulas contratuais modelo aprovadas pela RIPD expressam duas alternativas práticas habituais de uma transferência internacional, quais sejam, entre controladores e entre controladores e operadores. Além disso, a AAIP assinala que as cláusulas contratuais modelo são compatíveis com as cláusulas-padrão contratuais aprovadas pela *Disposición* nº 60/2016 e têm o potencial de contribuir para a convergência normativa para uma proteção de dados adequada, seguindo padrões mundialmente aceitos. Portanto, para promover a transferência de dados pessoais a partir da Argentina para jurisdições não adequadas, é possível empregar as cláusulas-padrão contratuais aprovadas pela *Disposición* nº 60/2016 ou as cláusulas contratuais modelo aprovadas pela RIPD.

---

[464] URCDP; AAIP. **Guía de Evaluación de Impacto en la Protección de Dato**s. 2020 Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-evaluacion-impacto-proteccion-datos. Acesso em: 2 nov. 2023.

[465] AAIP. Resolución nº 198/2023: **Modelo Para Transferencias Internacionales - Clausulas Contractuales**. 18 out. 2023(e). Disponível em: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-198-2023-391538. Acesso em: 2 nov. 2023.

3.3.1.4. Normas Corporativas Vinculantes

Ainda, nos termos do Decreto nº 1.558/2001, a transferência internacional terá nível de proteção adequado quando tal proteção advir de sistemas de autorregulação. De acordo com a *Resolución* nº 159, de 2018, a AAIP reconhece que, no cenário internacional, tem se tornado cada vez mais difundido o desenvolvimento de normas de autorregulação entre as entidades multinacionais pertencentes ao mesmo grupo econômico, na forma de normas corporativas vinculantes (NCV).[466]

Alinhado a esse movimento, a AAIP aprovou o Anexo I da *Resolución* nº 159/2018, sob o título *Lineamientos y Contenidos Básicos de Normas Corporativas Vinculantes*. O documento fornece orientações e requisitos mínimos para a elaboração das NVC por empresas que integram o mesmo grupo econômico, notadamente quando o país de destino não possui legislação adequada de proteção de dados. Segundo a AAIP, as diretrizes são úteis para assegurar os direitos dos titulares, proporcionar maior segurança jurídica em sistemas regulatórios complexos e, por sua vez, oferecer às empresas uma ferramenta mais dinâmica para cumprir os regulamentos em matéria de proteção de dados.

Nos termos das diretrizes, as NVC devem ser obrigatórias e exequíveis para as empresas que integrem um grupo econômico, bem como para empregados, subcontratados e terceiros beneficiários, conforme definido na legislação argentina, além de prever recursos judiciais e administrativos independentes, eficazes e acessíveis. No contexto das NVC, serão consideradas pertencentes ao mesmo grupo econômico as sociedades que sejam controladoras, controladas e aquelas vinculadas em que há influência significativa nas decisões, nome, domicílio, atividade principal, participação acionária, percentual de votos e, para as sociedades controladoras, os principais acionistas.

Com relação ao conteúdo básico, as NVC deverão incorporar os seguintes requisitos, cuja interpretação deverá ocorrer de acordo com o alcance e definições previstos na Lei nº 25.326/2000 ou em outras normas que venham a substituí-la:

> (1) condições de legalidade, incluindo princípios, direitos dos titulares e restrições para transferências ulteriores para países terceiros que não possuem nível adequado de proteção de dados;

[466] AAIP. Resolución nº 159/2018**: Lineamientos y Contenidos Basicos de Normas Corporativas Vinculantes**. 5 dez. 2018. Disponível em: https://www.boletinoficial.gob.ar/detalleAviso/primera/197428/20181207. Acesso em: 2 nov. 2023.

> (2) proteções específicas que decorrem das categorias de dados ou de decisão baseada exclusivamente em tratamento automatizado;
>
> (3) designação da qualidade de terceiros beneficiários concedida ao titular dos dados e à AAIP para exercício de suas prerrogativas, direitos e garantias;
>
> (4) adequado reconhecimento e estruturação dos procedimentos para o exercício dos direitos dos titulares dos dados;
>
> (5) possibilidade de o titular dos dados apresentar uma reclamação judicial ou administrativa no seu foro local;
>
> (6) imposição de responsabilidade solidária para as empresas que participam do tratamento de dados pessoais perante o titular dos dados e a autoridade supervisora em razão de qualquer violação da norma de autorregulação;
>
> (7) garantia de que a AAIP possa intervir quando a empresa que exportar os dados pessoais estiver estabelecida na Argentina e, na qualidade de terceiro beneficiário, quando se trata de dados pessoais de titulares residentes na Argentina. No âmbito da cooperação internacional entre autoridades supervisoras, garantia de que todas as autoridades dos países onde estão estabelecidas as empresas importadoras e exportadoras dos dados pessoais objeto da transferência possam intervir;
>
> (8) garantia de que as normas de autorregulação são efetivamente exigíveis das empresas do grupo pelo titular dos dados e pela AAIP;
>
> (9) garantia de capacitação contínua de funcionários relacionado às atividades de tratamento de dados pessoais (tradução livre).

As empresas que adotarem as NVC e seguirem as diretrizes indicadas na *Resolución* nº 159/2018 não têm a obrigação apresentá-las à AAIP para obtenção de aprovação formal. Do contrário, para efeitos de controle dos sistemas de autorregulação, as empresas que decidirem adotar normas de autorregulação que se diferem das diretrizes estabelecidas na *Resolución* nº 159/2018 deverão encaminhá-las para aprovação da AAIP, que poderá indicar o que falta para uma proteção adequada dos dados pessoais.

3.3.1.5. Exceções previstas na legislação argentina de proteção de dados

Nos termos do artigo 12 da Lei nº 25.326/2000, a proibição da transferência internacional de dados pessoais para países ou organizações que não ofereçam níveis de proteção adequados não se aplica no caso de cooperação jurídica internacional e de intercâmbio de dados médicos relativos à saúde, quando exigido pelo tratamento da pessoa afetada ou no âmbito de uma investigação epidemiológica. Além disso, o artigo contempla como exceções as transferências bancárias ou de ações, no que tange às respectivas operações e conforme a legislação aplicável. Também são consideradas exceções as situações que envolvem acordos no âmbito de tratados internacionais dos quais o Argentina seja parte. Por fim, o artigo estabelece como exceção a cooperação internacional entre agências de inteligência para combater o crime organizado, o terrorismo e o tráfico de drogas.

O artigo 12 do Decreto nº 1558/2001 alargou o catálogo das exceções e admite situações de transferência de dados pessoais para além das fronteiras baseadas no consentimento do titular e quando abrangem dados provenientes de registros públicos legalmente constituídos para facilitar o fornecimento de informações ao público e que estejam abertos à consulta pelo público em geral ou por qualquer pessoa que possa demonstrar um interesse legítimo, desde que, em cada caso particular, sejam cumpridas as condições legais e regulamentares para a consulta.[467]

3.3.2. Uruguai

No Uruguai, a Lei nº 18.331/2008 em conjunto com o Decreto n° 414/2009 preveem três regimes que permitem a realização de transferência internacional de dados pessoais. Primeiro, o país destinatário dos dados oferece nível de proteção adequado, de acordo com a avaliação da URCDP. Segundo, a URCDP autoriza a transferência quando o controlador oferecer garantias suficientes em relação à proteção de dados e aos direitos dos titulares. Terceiro, a transferência se enquadra nas exceções previstas na Lei nº 18.331/2008. Adicionalmente, os regulamentos formulados pela URCDP servem como complemento às situações já contempladas na legislação uruguaia.

Alinhado ao conceito de transferência internacional de dados, analisado na Seção 3.1, o Decreto n° 414/2009 define que os agentes envolvidos em uma transferência internacional de dados pessoais constituem o exportador e o importador. O exportador é a pessoa física ou jurídica, pública ou privada, localizada, no Uruguai, que realiza, de acordo com o previsto na legislação de proteção de dados pessoais uruguaia, uma transferência de dados pessoais para outro país. O importador é a pessoa física ou jurídica, pública ou privada, destinatária dos dados, que está localizada fora do território uruguaio.

3.3.2.1. Nível adequado de proteção de dados do país terceiro

O artigo 23 da Lei nº 18.331/2008 proíbe transferências internacionais de dados pessoais de qualquer tipo para países ou organizações que não ofereçam níveis de proteção adequados aos padrões de Direito Internacional ou regionais sobre a matéria, o que deve ser avaliados pela URCDP, considerando a conformidade das leis do país terceiro com os princípios e direitos de proteção de dados. Assim, a avaliação da

[467] ASOCIACIÓN POR LOS DERECHOS CIVILES - ADC. **El Sistema de Protección de Datos Personales en América Latina**. Ciudad de Buenos Aires, 30 dez. 2016. E-book. Disponível em: https://adc.org.ar/informes/sistema-proteccion-datos-personales-latam/. Acesso em: 2 nov. 2023.

adequação do país terceiro pela URCDP utiliza os parâmetros de Direito Internacional e regionais de proteção de dados, sobretudo os princípios e os direitos assegurados aos titulares.

A URCDP publicou a *Resolución* nº 23, de 2021, com a lista de países considerados com níveis de proteção adequados.[468] Para essa avaliação, foram considerados especialmente os Padrões de Proteção de Dados Pessoais emitidos pela RIPD e o RGPD. Nesse particular, a URCDP entende que os países membros da UE cumprem as normas internacionais em matéria de proteção de dados no âmbito do RGPD. Como consequência, a URCDP assume, expressamente, que os países terceiros ou organizações reconhecidos pelas decisões de adequação dos órgãos europeus têm um nível de proteção adequado. Quaisquer limitações ou exceções previstas nas decisões de adequação correspondentes também deverão ser consideradas como incluídas na *Resolución* nº 23/2021 da URCDP.

Por essa razão, alinhada à decisão do TJUE que invalidou o *Privacy Shield*, a URCDP reavaliou as transferências internacionais de dados pessoais para os EUA, anteriormente reconhecidas por conferirem nível de proteção adequado por meio da *Resolución* nº 4 de 2019,[469] e passou a exigir que fossem justificadas pelos demais mecanismos de transferência internacional previstos na legislação de proteção de dados uruguaia, incluindo as exceções descritas na Lei nº 18.331/2008 e, conforme aplicável, a autorização expressa da URCDP.[470] O objetivo claro dessa reavaliação foi assegurar que o Uruguai estivesse atualizado com o RGPD e os Padrões Ibero-americanos da RIPD, de forma que o país mantivesse sua conformidade com os critérios europeus.[471]

---

[468] URCDP. Resolución nº 23/2021: **se resuelve sobre la necesidad de actualizar la Resolución Nº 4/019, de 12 de marzo de 2019, sobre los países u organizaciones consideradas adecuadas para las transferencias internacionales de datos, de conformidad con lo establecido por el artículo 23 de la Ley Nº 18.331, de 11 de agosto de 2008**. 8 jun. 2021. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-23021. Acesso em: 2 nov. 2023.

[469] URCDP. Resolución nº 4/2019: **Se resuelve sobre los países adecuados para transferencias internacionales de datos, sustituyendo la Resolución N° 17/009, de 12 de junio de 2009**. 12 mar. 2019. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-4019 . Acesso em: 2 nov. 2023.

[470] URCDP. Resolución nº 23/2021: **se resuelve sobre la necesidad de actualizar la Resolución Nº 4/019, de 12 de marzo de 2019, sobre los países u organizaciones consideradas adecuadas para las transferencias internacionales de datos, de conformidad con lo establecido por el artículo 23 de la Ley Nº 18.331, de 11 de agosto de 2008**. 8 jun 2021. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-23021. Acesso em: 2 nov. 2023.

[471] BELLI, et. al. 2023. p. 43

A URCDP ressaltou que, nas transferências para os EUA, seriam especialmente valorizadas a implementação de cláusulas contratuais apropriadas, a localização de importadores em Estados norte-americanos que possuem normas de proteção de dados em vigor e a adoção do esquema de autocertificação disponibilizado pela FTC. Para agentes que apoiavam suas transferências internacionais de dados pessoais no *Privacy Shield*, a *Resolución* nº 23/2021 concedeu o prazo para as devidas adaptações.

A partir dessas premissas, e até a data de conclusão desta pesquisa, a *Resolución* nº 23/2021 determina que os seguintes países são considerados adequados para transferências internacionais de dados, uma vez que, no entender da URCDP, possuem normas de proteção de dados e meios para assegurar sua efetiva aplicação: membros da UE e do Espaço Econômico Europeu, o Principado de Andorra, a Argentina, o setor privado do Canadá, Guernsey, a Ilha de Man, as Ilhas Faroé, o Estado de Israel, Japão, Jersey, Nova Zelândia, Reino Unido da Grã-Bretanha e Irlanda do Norte e Suíça. A URCDP pode ampliar ou reduzir a lista de países ou organizações e, por isso, recomenda que exportadores e importadores revisem as condições da transferência antes de realizá-la, para garantir a sua conformidade.[472]

3.3.2.2. Autorização da URCDP

Da mesma forma, o art. 23 da Lei nº 18.331/2008 estabelece que a URCDP pode autorizar uma transferência ou uma série de transferências internacionais de dados pessoais para países terceiros que não possuem níveis de proteção adequados quando forem oferecidas garantias suficientes em relação à proteção da vida privada, dos direitos e liberdades fundamentais dos titulares e do exercício desses direitos. Tais garantias podem derivar de cláusulas contratuais apropriadas. A *Resolución* nº 41 de 2021 apresenta diretrizes sobre o conteúdo mínimo de cláusulas comuns para transferências entre todos os tipos de exportadores e importadores, bem como diretrizes para cláusulas específicas aplicáveis às transferências no âmbito de arranjos controlador-controlador, controlador-operador e operador-operador.[473] Apesar de serem aplicáveis às transferências de dados pessoais realizadas para países que não são adequados, a URCDP incentiva que os agentes

[472] URCDP. **Guía General de Protección de Datos Personales en Uruguay**. 2022. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-general-proteccion-datos-personales-uruguay. Acesso em: 2 nov. 2023.

[473] URCDP. Resolución nº 41/2021**. se resuelve sobre lo dispuesto por el artículo 23 de la Ley N° 18.331, de 11 de agosto de 2008 respecto a las transferencias internacionales a territorios no adecuados.** 8 set. 2021. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-41021. Acesso em: 2 nov. 2023.

considerem as cláusulas em todos os tipos de transferência internacional, quando pertinente.

As cláusulas comuns disciplinam, entre outros aspectos, a finalidade que se busca com a transferência pretendida; a instituição da legislação uruguaia e a identificação da URCPD para reger as cláusulas; a lista de dados transferidos e, no caso de dados sensíveis, o conteúdo e a finalidade da transferência de cada dado; as condições para viabilizar as transferências ulteriores de dados a partir do destino do importador; os direitos dos titulares; as operações específicas de tratamento a serem realizadas e as medidas de segurança necessárias para atender ao princípio da segurança de dados e da responsabilidade proativa; a possibilidade de previsão de mecanismos específicos para a resolução de litígios; a necessidade de cumprimento de medidas prévias de responsabilidade proativa na forma de avaliação de impacto à proteção de dados; as condições de guarda da documentação; obrigações de confidencialidade assumidas pelos colaboradores do importador e do exportador; e as condições para a divulgação de dados para autoridades estrangeiras.

As cláusulas aplicáveis às transferências entre controladores incluem: indicar a base legal que justifica a transferência, nos termos legislação uruguaia; indicar a base legal que justifica o tratamento que se pretende realizar, nos termos da legislação uruguaia; a determinação de que a responsabilidade solidária deverá ser aplicável e, em nenhum caso, pode implicar que seja vedada a reclamação do titular ao controlador localizado em território uruguaio; fornecer as condições para a contratação de operador pelo importador dos dados; estabelecer mecanismo de comunicação de incidente de segurança aos titulares e à URCDP, observadas as condições e prazos estabelecidos na legislação uruguaia.

As cláusulas aplicáveis às transferências entre controladores e operadores incluem: estabelecer o prazo específico de conservação dos dados, que não pode exceder a finalidade almejada, e os meios para a sua devolução e eliminação; estabelecer mecanismo de comunicação imediata ao controlador por incidentes de segurança e, eventualmente, estabelecer a obrigatoriedade de comunicação direta à URCDP; a determinação de que a contratação de suboperadores deve ser proibida, salvo com autorização expressa do controlador, o que também deve ser comunicado aos titulares; prever mecanismos para resposta ao exercício de direitos pelos titulares diante dos operadores; a previsão de que o controlador não pode se eximir de sua responsabilidade

pelos atos do operador, sem prejuízo da responsabilidade direta que possa recair sobre o operador em caso de violação do disposto na legislação uruguaia.

A cláusula aplicável às transferências entre operadores requer que a transferência internacional de dados pessoais para outros operadores seja realizada no âmbito de um contrato prévio com o controlador e nos limites nele estabelecidos, que devem ser juntados na forma de anexo ou referenciados nas respetivas cláusulas. O contrato deverá conter, no mínimo, as disposições para contratos entre controladores e operadores, que se estendem aos suboperadores, no que couber.

Ressalte-se que, com base no disposto no artigo 6º do Decreto nº 64/2020, qualquer transferência para país ou organização que não possui nível de proteção adequado deve ser precedida de uma avaliação de impacto da transferência, que funciona como um mecanismo preventivo para minimizar e, possivelmente, eliminar danos prováveis à privacidade dos titulares a partir da identificação e endereçamento dos riscos que as atividades habituais e/ou os novos projetos envolvendo o tratamento de dados pessoais da organização podem produzir.[474] Tal avaliação decorre do princípio da responsabilidade proativa, previsto no artigo 12 da Lei nº 18.331/2008, modificado pela Lei nº 19.670/2018, segundo o qual os controladores e operadores devem ir além do simples cumprimento da legislação de proteção de dados uruguaia e adotar medidas de forma autônoma capazes de demonstrar o efetivo cumprimento da norma quando requerido pela URCDP.

Nos termos do artigo 7º do Decreto nº 64/2020, a avaliação de impacto à proteção de dados pessoais deverá conter, no mínimo: a descrição sistemática do tratamento a ser realizado e sua finalidade; a avaliação do tratamento em relação ao cumprimento da legislação de proteção de dados uruguaia; a avaliação dos riscos para os direitos dos titulares; detalhes sobre as medidas de segurança e dos mecanismos de demonstração do cumprimento da legislação de proteção de dados uruguaia. Caso o resultado da avaliação apresente risco potencial e significativo para os direitos dos titulares, os agentes deverão dar conhecimento à URCDP e fornecer informações detalhadas sobre as medidas adotadas ou a serem adotadas para mitigá-lo e, neste último, o respectivo prazo. Em função do tipo ou volume dos dados e do seu tratamento, a URCDP poderá estabelecer critérios que contribuam para a avaliação.

---

[474] URCDP.**Guía General de Protección de Datos Personales en Uruguay**. 2022. p. 16. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-general-proteccion-datos-personales-uruguay. Acesso em: 2 nov. 2023.

Além desses requisitos, a URCDP e a AAIP elaboraram em cooperação o *Guia de Evaluación de Impacto en la Protección de Datos,* que visa a descrever as etapas que devem ser consideradas para a implementação da avaliação.[475] Para tanto, as autoridades basearam-se em legislações e guias sobre o assunto, com especial atenção à UE e às Convenções 108 e 108+ do Conselho da Europa.[476] Antes de iniciar a avaliação, recomenda-se que a organização considere potenciais riscos tanto na sua dimensão individual quanto na dimensão coletiva, uma vez que podem existir operações de tratamento de dados que, quando consideradas individualmente, não se afiguram relevantes, mas, quando avaliada no seu conjunto, podem constituir risco significativo para os direitos e garantias fundamentais dos titulares.[477] No caso das transferências internacionais de dados pessoais respaldadas por instrumentos contratuais, é importante avaliar o alcance das obrigações das partes, as categorias de dados que serão transferidas e as finalidades pretendidas, o destino dos dados e os mecanismos de eliminação dos dados, uma vez finalizado o contrato.[478]

Quando o agente entende que dispõe de garantias suficientes, o procedimento para requerer autorização à URCDP é regido pelos artigos 34 e 35 Decreto n° 414/2009. O requerimento terá início a pedido do exportador e deverá conter a identificação da base de dados, seu código de inscrição no Registo de Bases de Dados Pessoais, a descrição da transferência e da finalidade que a justifica, juntamente com a documentação comprobatória. Caso a autorização se baseie na existência de um contrato entre o exportador e o importador, deverá ser apresentada uma cópia do mesmo. Em 2023, a URCDP passou a disponibilizar um canal em seu *website* para requerer a autorização, de modo a facilitar o procedimento.[479]

Ainda, as transferências internacionais realizadas no âmbito de empresas multinacionais somente podem ocorrer entre a matriz, suas subsidiárias e/ou filiais, quando tiverem códigos de conduta devidamente registrados perante a URCDP. O requerimento terá início a pedido do controlador da base de dados e deve ser acompanhado de documentos, como a identificação da instituição, do código de conduta

---

[475] URCDP; AAIP. **Guía de Evaluación de Impacto en la Protección de Dato**s. 2020 Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-evaluacion-impacto-proteccion-datos. Acesso em: 2 nov. 2023.

[476] URCDP; AAIP, 2020. p. 3

[477] URCDP; AAIP, 2020. p. 6.

[478] URCDP; AAIP, 2020. p. 19.

[479] URCDP. **Solicitud de transferencias Internacionales**. 29 set. 2023. https://www.gub.uy/tramites/solicitud-transferencias-internacionales. Acesso em: 2 nov. 2023.

e seu responsável, além do conteúdo desse código, nos termos do artigo 35 e 36 do Decreto n° 414/2009.

3.3.2.3. Cláusulas Contratuais Modelo aprovadas pela RIPD

A URCDP aprovou a *Resolución* n° 50, de 2022, que admite o uso das cláusulas contratuais modelo aprovadas pela RIPD, incluídas no Guia de Implementação de Cláusulas Contratuais Modelo, para realizar transferências internacionais de dados pessoais a partir do Uruguai para jurisdições não adequadas, com as adaptações que os agentes considerarem apropriadas para sua conformidade com a legislação uruguaia, exceto nos casos em que as cláusulas contratuais modelo ofereçam maiores garantias aos titulares dos dados. A URCDP ressalta que o uso das cláusulas contratuais modelo não exclui a autorização da Unidade para a transferência que se pretende realizar.[480]

3.3.2.4. Exceções previstas na legislação uruguaia de proteção de dados

O artigo 23 da Lei nº 18.331/2008 prevê exceções para regra geral que proíbe a transferência de dados para países que não possuem nível adequado de proteção. Elas incluem a cooperação jurídica internacional e o intercâmbio de dados médicos, quando exigido pelo tratamento do titular por motivos de saúde ou questões de higiene pública. Além disso, o artigo contempla transferências bancárias ou de ações no que tange às respectivas operações e conforme a legislação aplicável. Também são consideradas exceções as situações que envolvem acordos no âmbito de tratados internacionais dos quais o Uruguai seja parte. Ainda, o artigo estabelece a cooperação internacional entre agências de inteligência para combater o crime organizado, o terrorismo e o tráfico de drogas, como uma exceção.

As exceções acima também foram identificadas na legislação argentina. Por seu turno, o artigo 23 da Lei nº 18.331/2008 prevê outras exceções quando o titular dos dados fornece seu consentimento inequívoco para a transferência pretendida ou quando a transferência é necessária para a execução de um contrato entre o titular e o agente, ou para diligências pré-contratuais a pedido do titular. Além disso, o artigo permite a transferência de dados para a execução ou celebração de um contrato entre o agente e um

[480] URCDP. Resolución n° 50/2022**. Se resuelve sobre la publicación de la "Guía de Implementación de Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales (TIPD)" por la Red Iberoamericana de Protección de Datos (RIPD)**. 29 nov. 2022. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-50022. Acesso em: 2 nov. 2023.

terceiro, desde que seja no interesse do titular dos dados. Também é admitida a transferência quando há uma necessidade ou exigência legal para a salvaguarda de um interesse público relevante, ou para o reconhecimento, exercício ou defesa de um direito em processo judicial. A salvaguarda de um interesse vital do titular dos dados é outra condição que justifica a transferência internacional de dados. Finalmente, o artigo prevê a possibilidade de transferência de dados oriundos de registros que, por força de disposição legal ou regulamentar, destina-se à prestação de informação ao público e esteja aberto à consulta pública ou de qualquer pessoa que demonstre interesse legítimo e que cumpra as condições legais para sua consulta.

3.3.3. Colômbia

Na Colômbia, como analisado na Seção 3.1, a terminologia para se referir à exportação de dados pessoais para países terceiros difere quando ocorre no âmbito de um arranjo controlador-controlador (situação denominada de transferência) ou controlador-operador (situação denominada de transmissão).

Para as transferências internacionais de dados pessoais, a Lei nº 1.581/2012 e o Decreto nº 1.377/2013 estabelecem quatro regimes que autorizam a operação. Primeiro, o país destinatário dos dados oferece nível de proteção adequado, de acordo com os parâmetros fixadas pela SIC. Segundo, os controladores integrantes de um mesmo grupo empresarial implementaram normas corporativas vinculantes aprovadas e certificadas pela SIC. Terceiro, a transferência se enquadra nas exceções previstas na Lei nº 1.581/2012. Quarto, a SIC emite uma declaração de conformidade quanto à viabilidade da transferência internacional. Para as transmissões internacionais de dados pessoais entre controladores e operadores, é necessário firmar um contrato de transmissão de dados, nos termos do Decreto nº 1.377/2013. Ainda, a sentença C-748 de 2011 da Corte Constitucional da Colômbia e as regulamentações e orientações publicados pela SIC, especialmente no Título V da Circular Única destinado à proteção de dados, conferem parâmetros e diretrizes que devem ser observados pelos agentes para complementar as regras previstas na legislação.

3.3.3.1. Nível adequado de proteção de dados do país terceiro

O tratamento dos dados pessoais objeto da transferência requer a observância dos requisitos previstos na legislação de proteção de dados colombiana, incluindo a

obtenção do consentimento do titular, quando necessário. Nas transferências internacionais de qualquer tipo, que ocorrem entre controladores, o artigo 26 da Lei nº 1.581/2012 proíbe que os dados sejam transferidos para países que não forneçam níveis de proteção adequados. A Lei nº 1.581/2012 determina que compete à SIC estabelecer os parâmetros para a definição de nível adequado de proteção, que não podem ser inferiores à proteção da legislação colombiana.

De início, a Corte Constitucional da Colômbia, por meio da Sentença C-748 de 2011, endereçou as condições que devem ser consideradas pela SIC para avaliar o nível de proteção de um país terceiro. A Corte determinou que a legislação do país terceiro deve ter princípios que compreendam as obrigações e direitos das partes envolvidas (titular dos dados, autoridades públicas, empresas, agências ou outros organismos que realizem o tratamento de dados pessoais) e dos dados (qualidade da informação, segurança técnica), além de um procedimento de proteção de dados que envolva mecanismos e autoridades que efetivem a proteção.

Alinhado ao entendimento da Corte Constitucional, o Título V da Circular Única da SIC estabelece os parâmetros para avaliação do nível de país terceiro, que incluem: a existência de normas aplicáveis ao tratamento de dados pessoais; o reconhecimento normativo de princípios aplicáveis ao tratamento de dados, que incluem os princípios da legalidade, finalidade, liberdade, veracidade ou qualidade dos dados, transparência, acesso e circulação restrita, segurança e confidencialidade; o reconhecimento normativo dos direitos dos titulares; o reconhecimento normativo dos deveres de controladores e operadores dos dados; a existência de meios e vias judiciais e administrativas para garantir a proteção efetiva dos direitos dos titulares e para exigir o cumprimento da lei; a existência de autoridade(s) pública(s) para fiscalizar o tratamento de dados pessoais, o cumprimento da legislação aplicável e a proteção dos direitos dos titulares, que exerça(m) efetivamente as suas funções. [481]

O Título V da Circular Única da SIC, igualmente, apresenta a lista de países considerados com nível adequado de proteção, que vem sendo atualizada ao longo dos anos e pode ser revista. Até a data de conclusão desta pesquisa, a lista compreende os seguintes países: Alemanha; Austrália, Áustria; Bélgica; Bulgária; Chipre; Costa Rica; Croácia; Dinamarca; Eslováquia; Eslovênia; Estônia; Espanha; Estados Unidos da

[481] SIC. **Título V Protección de Datos Circular Única**. 2022. p. 25. Disponível em: https://www.sic.gov.co/sites/default/files/normatividad/092022/T%C3%ADtulo%20V%20Versión%2029-09-2022.pdf. Acesso em: 2 nov. 2023.

América; Finlândia; França; Grécia; Hungria; Irlanda; Islândia; Itália; Japão; Letônia; Lituânia; Luxemburgo; Malta; México; Noruega; Países Baixos; Peru; Polônia; Portugal; Reino Unido; República Tcheca; República da Coreia; Romênia; Sérvia e Suécia. A SIC incorpora também os países que contam com decisão de adequação emitida pela Comissão Europeia (Suíça, Canadá, Argentina, Guernsey, Ilha de Man, Jersey, Ilhas Faroe, Andorra, Israel, Uruguai, Nova Zelândia e Japão).

Cabe destacar que o reconhecimento dos EUA como país adequado enfrentou opiniões por parte de especialistas, que mencionam que a conclusão não foi suficientemente fundamentada. De forma geral, destaca-se que outros países que conduziram essa avaliação concluíram que apenas algumas empresas e setores nos EUA atendem a critérios de adequação, desde que cumpram certos requisitos, mas não admitiram todo o território norte-americano.[482] Outra disposição prevista no Título V da Circular Única da SIC que também levantou debates, inclusive a respeito de sua validade, é a possibilidade de os próprios exportadores de dados avaliarem se certo país cumpre com os parâmetros de adequação, caso o país não seja catalogado pela SIC. Nelson Remolina aponta que essa situação não está estabelecida na Lei nº 1518/2012 e é uma extrapolação do poder regulamentar da SIC, que ampliou o conteúdo e alcance da lei, estabelecendo uma nova regra que não foi criada pelo legislador.[483]

3.3.3.2. Garantias adicionais para transferências internacionais

Ainda que as transferências de dados pessoais sejam realizadas para países que dispõem de um nível de proteção adequado reconhecido pela SIC, o Título V da Circular Única da SIC prevê que os controladores também devem ser capazes de demonstrar que observaram medidas apropriadas e eficazes para garantir o tratamento adequado dos dados pessoais transferidos e a segurança dos registros no momento da transferência, nos termos do princípio da responsabilidade demonstrada.[484]

Em linhas gerais, o princípio da responsabilidade demonstrada, que foi introduzido pelos artigos 26 e 27 do Decreto nº 1.377/2013, determina que os controladores deverão ser capazes de evidenciar, a pedido da SIC, a implementação de medidas apropriadas e eficazes para cumprir as obrigações da Lei nº 1.581/2012.

[482] BLANCO GAITAN, 2019. pp. 45-46.
[483] BELLI, et. al, 2023. p. 31.
[484] SIC. **Título V Protección de Datos Circular Única**. 2022. p. 25. Disponível em: https://www.sic.gov.co/sites/default/files/normatividad/092022/T%C3%ADtulo%20V%20Versión%2029-09-2022.pdf. Acesso em: 2 nov. 2023.

Aspectos particulares de cada organização devem ser considerados para a adoção de tais medidas, incluindo, entre outros, a natureza jurídica do agente e o porte do seu negócio, as categorias de dados tratados e os riscos para os titulares. As políticas internas da organização devem assegurar uma estrutura administrativa para a gestão dos dados, programas de treinamento e processos para endereçar consultas e reclamações dos titulares.[485]

À luz desses requisitos, a SIC publicou o *Guía para la Implementación del Principio de Responsabilidad Demostrada* para orientar os agentes a concretizarem o princípio em suas operações.[486] Segundo esse documento, o princípio privilegia a implementação de programas integrais de gestão de dados pessoais. A SIC poderá levar em consideração a adoção dos programas no momento de avaliar a imposição de uma sanção às organizações em caso de violação aos deveres e obrigações previstos na legislação colombiana. Para a SIC, isso acarreta benefício mútuo, uma vez que, de um lado, o controlador poderá demonstrar que eventual falha no tratamento de dados pessoais corresponde à situação isolada dentro de um programa robusto de governança de dados pessoais e, de outro, a SIC poderá investir esforços na fiscalização de agentes cuja atividade de tratamento de dados pessoais tem o potencial de ocasionar maior risco para os titulares.[487]

O *Guía para la Implementación del Principio de Responsabilidad Demostrada* prevê uma série de elementos essenciais que devem ser incorporados pela organização para desenvolver, implementar e dar continuidade aos programas integrais de gestão de dados pessoais, os quais incluem destinar recursos financeiros e de pessoal para efetivar o programa; estabelecer mecanismos internos para executar o programa e para auditá-lo; elaborar um inventário das bases de dados da organização e documentar políticas internas que estabeleçam regras que regem o tratamento de dados pessoais; instituir sistemas de administração de riscos associados ao tratamento de dados pessoais; realizar treinamentos periódicos para fins de conscientização de colaboradores a respeito das práticas adotadas pela organização que envolvem segurança e proteção de dados; implementar plano de resposta para endereçar eventuais violações à legislação de proteção de dados colombiana e incidentes de segurança; gerir operadores nos casos de

---

[485] Artigos 26 e 27, Decreto nº 1377/2013.

[486] SIC. **Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability)**. 2016. p. 26. Disponível em: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf. Acesso em: 2 nov. 2023.

[487] SIC, 2016. p.7.

transmissão internacionais de dados pessoais; desenvolver procedimentos para informar os titulares de forma clara e compreensível sobre como exercer os seus direitos.[488]

Mais recentemente, a SIC emitiu o *Guía para la Implementación del Principio de Responsabilidad Demostrada en las Transferencias Internacionales de Datos Personales*.[489] O documento propõe recomendações para que as organizações possam se adequar aos parâmetros colombianos de responsabilidade no contexto das transferências internacionais de dados, que devem ser examinados de acordo com as particularidades de cada exportação. Nesse cenário, os controladores devem demonstrar que adotaram medidas adequadas, úteis e práticas para alcançar dois principais objetivos, quais sejam, garantir o tratamento adequado dos dados pessoais que serão transferidos para outro país e conferir segurança aos registros de dados pessoais no momento de realização da transferência. A SIC elenca diversas recomendações voltadas para as transferências internacionais de dados pessoais que devem ser observadas para cumprir o princípio da responsabilidade demonstrada.

Previamente à exportação dos dados, a SIC recomenda que seja realizada uma avaliação de impacto à privacidade para gerenciar os riscos e garantir que os dados sejam tratados adequadamente. Essa avaliação deverá incluir, no mínimo, a descrição detalhada das operações de tratamento de dados pessoais envolvendo transferências internacionais; a avaliação dos riscos específicos para os direitos e liberdades dos titulares; e a identificação e classificação dos riscos, bem como a adoção de medidas para mitigá-los. Assim, identificar, medir, controlar e monitorar eventos ou situações que possam afetar a devida gestão de risco são elementos importantes para implementar o princípio da responsabilidade demonstrada.[490] A SIC é expressa ao advertir que o agente deve garantir que tem o direito de realizar a transferência internacional de dados pessoais, sob pena de responsabilização.[491]

A incorporação da privacidade, da ética e da segurança por padrão nas operações da organização igualmente constituem boas práticas para assegurar o correto tratamento de dados pessoais objeto de uma transferência internacional. Para a SIC, antes

---

[488] SIC, 2016. pp. 9-24.

[489] SIC. **Guía para la Implementación del Principio de Responsabilidad Demostrada en las Transferencias Internacionales de Datos Personales**. 2021. p. 24. Disponível em: https://www.sic.gov.co/sites/default/files/files/2021/2021%20Gu%C3%ADas%20para%20implementación%20del%20principio%20de%20responsabilidad%20demostrada%202021.pdf. Acesso em: 2 nov. 2023.

[490] SIC, 2021. p. 11.

[491] SIC, 2021. p 13.

da coleta dos dados, e ao longo do seu ciclo de tratamento, devem ser adotadas medidas preventivas de natureza diversa (tecnológica, organizacional, humana, processual, contratual entre outra) para evitar violações ao direito à privacidade, bem como falhas na segurança ou tratamento inadequado de dados pessoais. Essas medidas devem estar sujeitas a revisão, avaliação e melhorias contínuas.[492]

Além disso, conforme acima analisado, o princípio da responsabilidade demonstrada requer que os controladores sejam capazes de comprovar a implementação de medidas apropriadas e eficazes para cumprir as obrigações da legislação colombiana de proteção de dados. A SIC esclarece que as medidas apropriadas são aquelas adequadas às necessidades do tratamento, enquanto as medidas eficazes são aquelas que permitem que o resultado ou efeito desejado ou esperado seja alcançado. Portanto, os exportadores de dados devem estabelecer medidas adequadas, úteis, oportunas e eficientes, sujeitas à constante revisão e aprimoramento, para cumprir os requisitos legais de tratamento de dados pessoais. Para a SIC, é fundamental realizar treinamentos periódicos, capacitar os colaboradores e lhes fornecer as ferramentas necessárias para o desenvolvimento das operações envolvendo tratamento de dados pessoais.[493]

A SIC reforça que o tratamento adequado dos dados pessoais pressupõe que os direitos dos titulares sejam respeitados no país de destino e que o tratamento dos dados nesse país garanta o cumprimento dos princípios de proteção de dados estabelecidos pela legislação do país de origem, o que deve ser observado inclusive nas transferências ulteriores para outros países.[494] Também é recomendável replicar medidas proativas de tratamento de dados pessoais nas transferências internacionais, como periodicamente realizar atividades educacionais e treinamento específico para os colaboradores envolvidos na exportação de dados pessoais da organização; e assegurar, a depender do caso, que o controlador exportador possa monitorar o controlador importador para verificar o cumprimento adequado das suas obrigações.[495]

Ainda, a SIC destaca a importância de aprimorar a confiança e transparência com os titulares. A confiança se constrói na expectativa de que cada parte manterá seus compromissos e que ações positivas resultarão dessa relação. Nessa esteira, a transparência sobre como os dados pessoais são tratados se alia fortemente à confiança.

[492] SIC, 2021. p 12.
[493] SIC, 2021. p 14.
[494] SIC, 2021. p 15.
[495] SIC, 2021. p 16.

A SIC recomenda disponibilizar canais abertos de comunicação nos processos de transferência internacional de dados, implementar sistema para consultas e reclamações dos titulares e cumprir, na prática, os compromissos assumidos nas políticas de tratamento de dados.[496]

Por fim, a SIC recomenda que os agentes envolvidos nas transferências internacionais de dados celebrem contratos para regular as obrigações e responsabilidades de cada parte durante a transferência, os quais devem ser condizentes com as peculiaridades e necessidades da organização, considerando aspectos como a natureza, a quantidade de dados transferidos e quem terá acesso a eles; as medidas de segurança que o importador deverá cumprir; os mecanismos para exercício dos direitos que devem ser garantidos aos titulares; os princípios, as finalidades e o prazo em relação ao qual o importador dos dados poderá tratá-los; a possibilidade ou não de realizar transferências ulteriores para outros países e as condições que devem ser observadas nesses casos.

Adicionalmente, a SIC recomenda que sejam incluídas disposições contratuais relacionadas à fiscalização e responsabilização dos agentes, tais como estabelecer o agente que responderá perante as autoridades e os titulares dos dados por eventual tratamento indevido e danos causados, determinar o regime de responsabilidade dos agentes diante do titular por possíveis violações de seus direitos e danos causados, definir quem irá gerenciar incidentes de segurança que afetem dados pessoais, bem como quem é o responsável pela comunicação às autoridades e aos titulares dos dados. Tais instrumentos poderão ser considerados na declaração de conformidade da SIC, conforme será analisado adiante.

3.3.3.3. Normas Corporativas Vinculantes

Na forma do artigo 27 da Lei nº 1.581/2012, as Normas Corporativas Vinculantes (NCV) representam uma alternativa complementar, que autoriza a realização de transferências internacionais de dados pessoais entre controladores de um mesmo grupo empresarial que estejam localizados em países distintos. O conceito de grupo empresarial tem previsão no artigo 28 da Lei nº 222 de 1995 e envolve, além de vínculo de subordinação, unidade de propósito e direção entre as entidades integrantes, o qual se verifica quando a existência e as atividades de todas as entidades perseguem a consecução de um objetivo determinado pela matriz ou pela controladora, em razão da direção que

[496] SIC, 2021. p 19.

esta exerce sobre o todo, sem prejuízo do desenvolvimento individual do objeto social ou atividade de cada uma delas.[497]

O Decreto nº 255/2022 regulamenta as condições mínimas das NCV, incluindo as garantias, os mecanismos e os requisitos de proteção de dados que devem ser oferecidos, bem como os procedimentos para aprovação das normas de modo a obter a devida certificação.[498] As NCV materializam-se por meio de sistemas de autorregulação que conferem direitos e garantias aos titulares e obrigações ao grupo empresarial. Nesse sentido, as NCV são definidas como políticas, princípios de boa governança ou códigos de boas práticas, cujo cumprimento é obrigatório e assumido pelo controlador exportador estabelecido na Colômbia para realizar uma transferência ou um conjunto de transferências de dados pessoais para outro controlador importador que esteja localizado fora do território colombiano e que faça parte do mesmo grupo empresarial. Nesse caso, salvo quando estiver respaldado por outros mecanismos de transferências internacionais estabelecidos na legislação colombiana, a observância das NCV pelo grupo empresarial é obrigatória.[499]

Quanto às garantias e mecanismos de proteção de dados das NCV, o Decreto nº 255/2022 determina que os dados sejam tratadas de forma lícita, leal e transparente em relação aos titulares; coletados para fins determinados, explícitos e legítimos, não sendo posteriormente utilizados de forma incompatível com esses fins; adequados, pertinentes e limitados ao mínimo necessário para atender às finalidades; precisos e atualizados, mantendo medidas razoáveis para garantir que os dados pessoais imprecisos sejam prontamente excluídos ou corrigidos; conservados de forma a permitir a identificação do titular por período não superior ao necessário; tratados sob a gestão do controlador, o qual, para cada operação de tratamento, garantirá e demonstrará o cumprimento do disposto no Decreto.[500]

---

[497] COLOMBIA. Lei nº 222/1995. **Por la cual se modifica el Libro II del Código de Comercio, se expide un nuevo régimen de procesos concursales y se dictan otras disposiciones.** 20 dez. 1995. Disponível em: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6739. Acesso em: 2 nov. 2023.

[498] COLOMBIA. Decreto nº 255/2022**. Por el cual se adiciona la Sección 7 al Capítulo 25 del Título 2 de la Parte 2 del Libro 2 del Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, sobre normas corporativas vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países**. 23 fev. 2022. Diponível em: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=179087. Acesso em: 2 nov. 2023.

[499] Artigo 2.2.2.25.7.3, Decreto nº 255/2022.

[500] Artigo 2.2.2.25.7.4, Decreto nº 255/2022.

Ainda nos termos do Decreto nº 255/2022, as NCV deverão conter, no mínimo, os seguintes requisitos:[501]

> (1) a estrutura e dados de contato do grupo empresarial e de cada uma das entidades cujo cumprimento das NCV é obrigatório;
> (2) a transferência ou conjunto de transferências de dados, incluindo as categorias de dados pessoais, o tipo de tratamento e suas finalidades, os grupos titulares afetados e o nome do país terceiro ou países terceiros;
> (3) a natureza juridicamente vinculante para todas as entidades que integram o grupo empresarial;
> (4) a aplicação dos princípios gerais de proteção de dados estabelecidos na legislação colombiana;
> (5) a referência aos direitos dos titulares previstos na Lei nº 1.581/2012 e seus regulamentos, bem como os meios efetivos para exercê-los;
> (6) as medidas adotadas para evitar transferências para outras entidades que não pertençam ao grupo empresarial;
> (7) a referência aos responsáveis pelo cumprimento das NCV, bem como pela supervisão de treinamentos e pelo tratamento de eventuais reclamações dos titulares;
> (8) os mecanismos estabelecidos pelo grupo empresarial para assegurar a verificação do cumprimento das NCV, incluindo auditorias de proteção de dados e métodos para garantir ações corretivas para proteger os direitos do titular;
> (9) os mecanismos estabelecidos para comunicar e registrar as modificações introduzidas nas políticas e para notificá-las à SIC;
> (10) os treinamentos em matéria de proteção de dados destinados aos responsáveis que terão acesso permanente ou habitual aos dados pessoais transferidos;
> (11) os procedimentos para que os titulares possam realizar consultas ou apresentar reclamações e para que sejam endereçadas oportunamente de acordo com o disposto na Lei nº 1.581/2012;
> (12) a observância do princípio de responsabilidade demonstrada para comprovar a implementação de medidas úteis, pertinentes e eficazes para o cumprimento das NCVs, considerando as recomendações do *Guía para la Implementación del Principio de Responsabilidad Demostrada en las Transferencias Internacionales de Datos Personales*;
> (13) o período de vigência para as NCV (tradução livre).

A Corte Constitucional da Colômbia, na sentença C-748 de 2011, concluiu que, para que cumpram com seus objetivos, as NVC devem ser revisadas pela SIC. Seguindo o entendimento da Corte colombiana, o Decreto nº 255/2022 prevê que a SIC tem competência para revisar e aprovar as NCV. O processo de submissão exige que as NCV sejam apresentadas por uma entidade do grupo empresarial localizada na Colômbia. As NCV entrarão em vigor e poderão ser aplicadas a partir da data em que a SIC emitir a certificação. O grupo empresarial que conta com a aprovação das NCV pela SIC deverá informar tal situação em seu *website*.[502]

Em caso de alterações substanciais no conteúdo das NCV previamente aprovadas, é necessário notificar a SIC, que poderá expedir instruções sobre as medidas

[501] Artigo 2.2.2.25.7.5, Decreto nº 255/2022.
[502] Artigo. 2.2.2.25.7.6; Artigo 2.2.2.25.7.7, Decreto nº 255/2022.

e procedimentos para manter o nível de proteção oferecido. As empresas do grupo empresarial são solidariamente responsáveis pelo cumprimento das NCV e, consequentemente, a SIC poderá solicitar, investigar e sancionar o controlador estabelecido em território colombiano pelas infrações cometidas pelas entidades vinculadas.[503]

3.3.3.4. Exceções previstas na legislação colombiana de proteção de dados

Em que pese seja proibido transferir dados pessoais para países que não possuem níveis de proteção adequados, a Lei nº 1.581/2012 estabeleceu situações excepcionais para essa proibição. Tais exceções incluem as transferências de dados autorizadas pelos titulares. Também contemplam o intercâmbio de dados médicos, quando exigido pelo tratamento do titular por motivos de saúde ou questões de higiene pública. Adicionalmente, as transferências bancárias ou relacionadas ao mercado de ações, nos termos da legislação aplicável, são abrangidas. Outra exceção se dá em casos de transferências que estão sujeitas a acordos internacionais dos quais a Colômbia seja parte, baseando-se no princípio de reciprocidade. Além disso, são permitidas transferências necessárias à execução de um contrato entre o titular e o controlador ou para diligências pré-contratuais, desde que o titular tenha dado sua autorização. Por fim, são admitidas transferências legalmente exigidas para a salvaguarda do interesse público ou para o reconhecimento, exercício ou defesa de um direito em processo judicial.

3.3.3.5. Decisão de conformidade da SIC

Caso o país não ofereça nível de proteção adequado e a transferência não esteja contemplada em uma das exceções previstas na Lei nº 1.581/2012, ainda é possível realizar a exportação dos dados mediante a emissão de uma declaração de conformidade, pela SIC. Trata-se de hipótese prevista no parágrafo primeiro do art. 26 da Lei nº 1.581/2012, que também confere poderes à SIC para solicitar informações e realizar procedimentos para apurar o cumprimento dos pressupostos necessários para viabilizar a transferência.

Conforme o Título V da Circular Única da SIC, para solicitar a declaração de conformidade, o controlador deverá apresentar o pedido à SIC e fornecer as informações e documentos elencados no *Guía para Solicitar la Declaración de Conformidad sobre*

[503] Artigo. 2.2.2.25.7.4, Decreto nº 255/2022.

las Transferencias Internacionales de Datos Personales,[504] que não apenas devem ser submetidos em sua totalidade, como também traduzidos para a língua espanhola. Eles incluem:

> (1) nome e finalidades das bases de dados do controlador que contêm dados pessoais objeto da transferência;
> (2) tratamento conferido aos dados pessoais presentes em tais bases de dados;
> (3) categorias de dados pessoais que serão objeto da transferência internacional entre o controlador exportador e o controlador importador, identificando se incluem dados sensíveis ou dados de menores de idade;
> (4) cópia das políticas de tratamento de dados pessoais do controlador exportador;
> (5) nome e razão social do controlador importador;
> (6) cópia do documento que comprova a existência e representação legal do controlador importador;
> (7) cópia do contrato ou instrumento jurídico que descreve as condições da transferência de dados pessoais, em particular, as garantias relacionadas à proteção de dados pessoais objeto da transferência;
> (8) medidas de segurança e confidencialidade previstas para realizar a transferência;
> (9) tratamento conferido aos dados pessoais transferidos ao controlador importador;
> (10) finalidade das bases de dados do controlador importador e daquelas em que serão armazenados os dados transferidos da Colômbia;
> (11) cópia da política de tratamento de dados pessoais do controlador importador;
> (12) cópia da política e segurança da informação do controlador importador e, caso não a tenha, as medidas técnicas, humanas e administrativas implementadas para o tratamento de dados pessoais objeto da transferência;
> (13) mecanismos ou canais implementados pelo controlador importador para receber as consultas e reclamações dos titulares;
> (14) período de armazenamento dos dados pessoais nas bases de dados do controlador importador;
> (15) tratamento que será dado aos dados, uma vez que se atenda a finalidade para a qual foi realizada a transferência;
> (16) categorias das pessoas naturais ou jurídicas que poderão acessar os dados pessoais objeto da transferência (empregados, parceiros comerciais, autoridades) e cópia dos modelos das cláusulas ou acordos de confidencialidade implementados pelo controlador importador;
> (17) cópia da lei de proteção de dados pessoais do país destinatário;
> (18) cópia da lei ou norma mediante a qual se confere os poderes e atribuições da autoridade de proteção de dados do país destinatário ou entidade que atue como tal;
> (19) último relatório publicado pela autoridade de proteção de dados do país destinatário para prestar contas do cumprimento de suas atribuições;
> (20) mecanismos existentes no país destinatário para garantir a proteção dos dados pessoais dos titulares, as autoridades administrativas ou judiciais em relação às quais os titulares podem apresentar reclamações e denúncias, e descrição do caráter gratuito ou oneroso de tais mecanismos;
> (21) qualquer outra informação ou documento que permita entender a transferência que se pretende realizar. Em qualquer caso, a SIC poderá requerer informações adicionais e realizar os procedimentos que considerar necessários (tradução livre).

[504] SIC. **Guía para Solicitar la Declaración de Conformidad sobre las Transferencias Internacionales de Datos Personales.** 2016. Disponível em: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Guia_para_solicitar_la_declaracion_de_conformidad_sobre_las_trasferencias_internacionales_de_datos_personales.pdf. Acesso em: 2 nov. 2023.

Após a solicitação, cabe à SIC examinar se foram apresentadas todas as informações e documentos exigidos, bem como avaliar se é possível determinar se a transferência garante o cumprimento dos princípios, dos direitos dos titulares e das obrigações do controlador importador, conforme a legislação de proteção de dados colombiana.

A despeito do procedimento acima analisado, o Título V da Circular Única da SIC igualmente prevê hipótese em que a operação pressupõe estar coberta por uma declaração de conformidade.[505] É o caso de quando o controlador exportador localizado na Colômbia, em atenção ao princípio da responsabilidade demonstrada, tenha firmado um contrato com o controlador importador ou implementado outro instrumento jurídico por meio do qual indica as condições que regem a transferência internacional de dados pessoais e que garantem o cumprimento dos princípios e das obrigações que lhes competem.

Os controladores poderão realizar a transferência internacional, desde que comuniquem previamente à SIC e declaram ter um contrato vigente ou outro instrumento jurídico que assegure a proteção dos dados pessoais objeto da transferência, o qual poderá estar sujeito à fiscalização da SIC a qualquer momento. Em caso de descumprimento, a SIC poderá instaurar investigação, impor sanções correspondentes e determinar as demais providências que se façam necessárias.

3.3.3.6. Transmissões internacionais de dados pessoais entre controladores e operadores

As transmissões de dados pessoais não foram contempladas inicialmente pela Lei nº 1.581/2012, tendo sido regulamentadas pelo Decreto nº 1.377/2013. Elas representam uma classe especial de transferência que se refere à comunicação de dados pessoais entre um controlador e um operador, seja dentro ou fora da Colômbia. Nas transmissões internacionais, os dados são transmitidos para um operador localizado em um país terceiro.

O contrato de transmissão de dados pessoais é o instrumento por meio do qual as partes estabelecem as obrigações que o operador assumirá para realizar o tratamento

[505] SIC. **Título V Protección de Datos Circular Única**. 2022. p. 25. Disponível em: https://www.sic.gov.co/sites/default/files/normatividad/092022/T%C3%ADtulo%20V%20Versión%2029-09-2022.pdf. Acesso em: 2 nov. 2023.

de dados em nome e sob as instruções do controlador.[506] O artigo 25 do Decreto nº 1.377/2013 determina as condições e obrigações legais que devem estar refletidos nesse arranjo contratual. O contrato deverá definir o escopo do tratamento, as atividades que o operador realizará em nome do controlador para tratar os dados pessoais e as obrigações do operador em relação aos titulares a ao controlador. Ainda, o operador deverá se comprometer a observar as obrigações previstas na política de tratamento de dados do controlador, a qual passará a integrar o contrato, além de realizar o tratamento de acordo com as finalidades que os titulares tenham autorizado e com a legislação colombiana.

Além disso, é necessário incluir no contrato, pelo menos, as seguintes obrigações para o operador: realizar o tratamento dos dados em nome do controlador e conforme os princípios que os tutelam; proteger a segurança das bases de dados que contêm dados pessoais, e manter a confidencialidade do tratamento dos dados pessoais. Conforme o artigo 24 do Decreto nº 1.377/2013, nas transmissões internacionais, não é necessário que o titular seja notificado ou forneça o seu consentimento quando existir um contrato. O Título V da Circular Única da SIC, por sua vez, determina que é possível realizar a transmissão de dados pessoais para os países que contam com um nível adequado de proteção de dados pessoais, nos termos que regem a transferência de dados pessoais.[507]

3.3.4. Brasil

No Brasil, a LGPD prevê três regimes que autorizam a realização de transferências internacionais de dados. Primeiro, o país ou organismo internacional destinatário dos dados possui nível de proteção de dados adequado, de acordo com a avaliação da ANPD. Segundo, o agente oferece e comprova a implementação de garantias de cumprimento dos preceitos da norma, na forma de cláusulas contratuais, que podem ser padrão ou específicas, normas corporativas globais, selos, certificados e códigos de conduta regularmente emitidos. Terceiro, a transferência enquadra-se nas exceções previstas pela LGPD.

---

[506] SIC. **Guía para la Implementación del Principio de Responsabilidad Demostrada en las Transferencias Internacionales de Datos Personales**. 2021. p. 24. Disponível em: https://www.sic.gov.co/sites/default/files/files/2021/2021%20Gu%C3%ADas%20para%20implementación%20del%20principio%20de%20responsabilidad%20demostrada%202021.pdf. Acesso em: 2 nov. 2023.

[507] SIC. **Título V Protección de Datos Circular Única**. 2022. p. 25. Disponível em: https://www.sic.gov.co/sites/default/files/normatividad/092022/T%C3%ADtulo%20V%20Versión%2029-09-2022.pdf. Acesso em: 2 nov. 2023.

No contexto das iniciativas de regulamentação da ANPD, em 2022, foi apresentada a Tomada de Subsídios nº 2, com o objetivo de receber contribuições da sociedade para regulamentar os regimes de tutela previstos na LGPD.[508] Durante essa iniciativa, a ANPD ressaltou que a formulação do regulamento sobre transferências internacionais de dados pessoais teria como prioridade a definição do conteúdo dos mecanismos cuja natureza é contratual, sob o argumento de que são consideradas soluções mais acessíveis e com menor custo de aplicação, tornando-se uma alternativa viável para pequenas e médias empresas.

Após a coleta de subsídios, em 2023, foi divulgada a proposta de regulamento de transferências internacionais de dados, que contempla os modelos de cláusulas-padrão contratuais, o fluxo de aprovação das cláusulas específicas e das normas corporativas globais.[509] Além dos instrumentos contratuais, a proposta de regulamento acabou por também estabelecer os critérios para a avaliação de uma decisão de adequação que devem ser considerados pela ANPD. O documento foi submetido à consulta pública e à audiência pública e, até a data de conclusão desta pesquisa, não foi publicada a sua versão definitiva. Contudo, considerando o avanço no tema, esta Subseção irá considerar as disposições previstas na proposta de regulamento.

Em consonância com o conceito de transferência internacional de dados analisado na Seção 3.1, nos termos da proposta de regulamento, o exportador é o agente de tratamento localizado no Brasil ou em país estrangeiro que transferirá os dados pessoais para um destinatário localizado em outro país, e o importador representa o agente de tratamento situado fora do território nacional que receberá esses dados do exportador.[510]

A proposta de regulamento requer a observância de diretrizes gerais aplicáveis a qualquer mecanismo de transferência internacional de dados pessoais, que incluem a adoção de medidas de responsabilização e prestação de contas, mediante o oferecimento e a comprovação de garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados pessoais previstos na LGPD, bem como a observância de procedimentos simples, interoperáveis e compatíveis com normas e boas

---

[508] ANPD. **Tomada de Subsídios sobre Transferência Internacional**. 2022(b). Disponível em: https://www.gov.br/participamaisbrasil/tomada-de-subsidios-transferencia-internacional. Acesso em: 2 nov. 2023.

[509] ANPD. **Aberta Consulta Pública sobre norma de transferências internacionais de dados pessoais**. 15 ago. 2023(b). Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/aberta-consulta-publica-sobre-norma-de-transferencias-internacionais-de-dados-pessoais. Acesso em: 2 nov. 2023.

[510] Artigo 3º, I e II, da proposta de regulamento de TIDP da ANPD.

práticas internacionais reconhecidas, e que promovam o desenvolvimento social e econômico e assegurem o livre fluxo transfronteiriço de dados pessoais com confiança e respeito aos direitos dos titulares.[511] Além dos mecanismos de transferência, os agentes deverão respaldar a operação em um base legal.[512]

Ao avaliar se a operação de tratamento compreende uma transferência internacional, os agentes deverão adotar medidas capazes de comprovar o cumprimento das normas de proteção de dados pessoais e a eficácia dessas medidas, de forma compatível com o grau de risco do tratamento e com a modalidade de transferência internacional utilizada.[513] Nesse sentido, a transferência internacional somente poderá ser realizada para atender a propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. Ainda, a transferência igualmente deverá se limitar ao mínimo de dados necessário para alcançar as suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.[514]

3.3.4.1. Nível adequado de proteção de dados do país terceiro

O artigo 33 da LGPD admite transferências internacionais de dados pessoais para países ou organismos internacionais que proporcionem nível adequado de proteção dados, o que deverá ser avaliado pela ANPD mediante uma decisão de adequação. Tal avaliação deverá considerar as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional, limitada à legislação diretamente aplicável ou que gere impactos relevantes sobre o tratamento de dados pessoais e os direitos dos titulares, podendo ser analisados, se necessário, regulamentos e normas complementares;[515] a natureza dos dados; a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos na LGPD;[516] a adoção de medidas de segurança; a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais, incluindo a existência e o efetivo funcionamento de uma entidade reguladora independente, com competência para assegurar o cumprimento das normas de proteção de dados e o respeito aos direitos dos titulares.[517]

---

[511] Artigo 2º, II e III, da proposta de regulamento de TIDP da ANPD.
[512] Artigo 9, caput, I, da proposta de regulamento de TIDP da ANPD.
[513] Artigo 4º, parágrafo 2º, da proposta de regulamento de TIDP da ANPD.
[514] Artigo 9, parágrafo único, da proposta de regulamento de TIDP da ANPD.
[515] Artigo 11, §1º, da proposta de regulamento de TIDP da ANPD.
[516] Artigo 11, §2º, da proposta de regulamento de TIDP da ANPD.
[517] Artigo 11, §3º, da proposta de regulamento de TIDP da ANPD.

Nos termos da proposta de regulamento, a avaliação do nível de proteção de dados conduzida pela ANPD deve contemplar os riscos e os benefícios proporcionados pela decisão de adequação, como a garantia dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD, além dos impactos sobre o fluxo internacional de dados, das relações diplomáticas e da cooperação internacional do Brasil, com outros países e organismos internacionais. Nesse sentido, a ANPD deve priorizar a avaliação do nível de proteção de dados de países estrangeiros ou organismos internacionais que garantam tratamento recíproco ao Brasil e cujo reconhecimento de adequação viabilize a ampliação do livre fluxo de transferências internacionais de dados pessoais entre os países.[518]

Com relação ao procedimento de emissão da decisão de adequação, a iniciativa poderá ser instaurada de ofício pelo Conselho Diretor da ANPD ou após solicitação das pessoas jurídicas de direito público referidas na Lei de Acesso à Informação (Lei nº 12.527/2011), as quais incluem entidades públicas integrantes da administração direta e indireta do Poder Executivo, do Poder Legislativo e do Poder Judiciário, além de empresas estatais.[519] Esse procedimento será instruído pela área técnica competente da ANPD, que se manifestará sobre o mérito da decisão, indicando, se for o caso, as condicionantes a serem observadas. O Ministério das Relações Exteriores do Brasil será cientificado da instauração do processo, podendo apresentar manifestação.[520]

A decisão de adequação deve ser formalizada por Resolução do Conselho Diretor da ANPD e publicado na página da Autoridade na Internet. O Conselho Diretor da ANPD, igualmente, poderá editar normas complementares sobre o procedimento de reavaliação periódica do nível de proteção e de revisão da decisão de adequação.[521] Como a publicação da versão definitiva da proposta de regulamento está pendente, a ANPD ainda não realizou a avaliação de adequação de qualquer país.

3.3.4.2. Garantias adicionais para transferências internacionais

Além da decisão de adequação, o artigo 33 da LGPD estabelece que as transferências internacionais de dados pessoais podem ser realizadas quando o

[518] Artigo 12, da proposta de regulamento de TIDP da ANPD.
[519] Artigo 13, I, da proposta de regulamento de TIDP da ANPD.
[520] Artigo 13, II, III, §1º, da proposta de regulamento de TIDP da ANPD.
[521] Artigo 13, §2º e 3º, da proposta de regulamento de TIDP da ANPD.

controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD na forma de cláusulas contratuais específicas para determinada transferência; cláusulas-padrão contratuais; normas corporativas globais; selos, certificados e códigos de conduta regularmente emitidos.

A verificação de tais instrumentos, bem como a definição do conteúdo das cláusulas contratuais padrão devem ser realizadss pela ANPD. A esse respeito, podem ser requeridas informações suplementares ou realizadas diligências relacionadas às operações de tratamento. Para a avaliação das garantias que assegurem o cumprimento dos princípios de proteção de dados e dos direitos do titular, também podem ser consideradas as medidas técnicas e organizacionais adotadas, desde a fase de concepção do produto ou serviço até a sua execução. Quaisquer alterações em tais garantias deverão ser comunicadas à ANPD.

Quanto aos selos, certificados e códigos de conduta, a ANPD poderá designar organismos de certificação para emissão dos documentos, que permanecerão sob a fiscalização da ANPD e, em caso de desconformidade com a LGPD, submetidos a revisão ou anulados. Os aspectos relacionados a esses mecanismos ainda estão pendentes de regulamentação, pela ANPD.

3.3.4.3. Cláusulas-padrão Contratuais

As cláusulas-padrão contratuais, elaboradas e aprovadas pela ANPD por meio da proposta de regulamento, estabelecem garantias mínimas e condições para a realização de transferência internacional de dados. A validade da transferência pressupõe a adoção integral e sem alteração do texto dessas cláusulas, que poderão ser utilizadas como parte de contrato especifico para reger a transferência internacional de dados ou incorporadas a um contrato de objeto mais amplo.[522] A esse respeito, eventuais cláusulas adicionais e as demais disposições previstas no instrumento contratual ou em contratos coligados firmados entre o exportador e o importador não poderão excluir, modificar ou contrariar, direta ou indiretamente, o disposto nas cláusulas-padrão contratuais.[523]

Para assegurar a transparência, o titular dos dados poderá solicitar ao agente designado nas cláusulas-padrão contratuais o instrumento contratual utilizado para a

[522] Artigo 14, art. 15, §1º, da proposta de regulamento de TIDP da ANPD.
[523] Artigo 15, §2º, da proposta de regulamento de TIDP da ANPD.

realização da transferência internacional, observados os segredos comercial e industrial. Ainda, o referido agente deverá publicar, em sua página na internet, documento contendo informações redigidas em língua portuguesa, em linguagem simples, clara, precisa e acessível, sobre a realização da transferência internacional de dados pessoais, incluindo, pelo menos, informações sobre a forma, a duração e a finalidade específica da transferência internacional; o país de destino dos dados transferidos; a identificação e os contatos do controlador; o uso compartilhado de dados pelo controlador e a finalidade; as responsabilidades dos agentes que realizarão o tratamento; e os direitos do titular e os meios para o seu exercício, incluindo canal de fácil acesso e o direito de peticionar contra o controlador perante a ANPD.[524]

Nos termos do Anexo II da proposta de regulamento, o conteúdo das cláusulas-padrão contratuais se dividem em seções.[525] Na seção 1, o exportador e o importador deverão indicar as informações gerais da transferência, incluindo a identificação das partes, definição do papel de controlador ou operador, a possibilidade de transferência ulteriores e o objeto da transferência, além de atribuir as responsabilidades da parte designada para cumprir obrigações específicas relativas à transparência, direitos dos titulares e comunicação de incidentes de segurança.

Já na seção II, estão dispostas as cláusulas mandatórias, que disciplinam, entre outros aspectos, a descrição e as finalidades da transferência; a instituição da legislação brasileira e supervisão da ANPD para reger as cláusulas; regras de interpretação das cláusulas; possibilidade adesão das cláusulas por terceiros; obrigações gerais do exportador e do importador; proteção especial para dados sensíveis e dados de crianças e adolescentes; garantia da legalidade e transparência dos dados; direitos dos titulares; comunicação de incidentes; responsabilização e ressarcimento de danos, salvaguardas para transferências posteriores; notificação sobre solicitações de acesso de autoridades; término de tratamento e eliminação de dados, medidas de segurança no tratamento de dados pessoais, consequências em razão do descumprimento das obrigações pelo importador; e o estabelecimento da jurisdição brasileira para dirimir disputas. Cabe destacar que as partes devem realizar a avaliação da legislação do país destinatário dos dados, de modo a declarar que não identificaram leis ou práticas administrativas que impeçam o importador de cumprir as obrigações assumidas.

[524] Artigo 16, da proposta de regulamento de TIDP da ANPD.
[525] Anexo II da proposta de regulamento de TIDP da ANPD.

Ainda, na seção III, deve ser incluído o detalhamento das medidas de segurança adotadas, tais como governança e supervisão de processos internos, medidas de segurança técnicas e administrativas, incluindo medidas para garantir a segurança das operações realizadas. Na seção IV, por sua vez, podem ser incluídas cláusulas adicionais e aditivos, a critério das partes, para disciplinar, questões de natureza comercial, a rescisão contratual, o prazo de vigência e eleição de foro no Brasil. Com a publicação da versão final da proposta de regulamento, os agentes de tratamento que elegerem as cláusulas-padrão contratuais para realizar a transferência internacional de dados deverão incorporá-las aos seus respectivos instrumentos contratuais.

3.3.4.4. Cláusulas-padrão Contratuais Equivalentes

A proposta de regulamento inaugurou um novo mecanismo de transferência internacional de dados, que estabelece a possibilidade de a ANPD reconhecer a equivalência de cláusulas-padrão contratuais de outros países ou de organismos internacionais. A previsão desse procedimento desonera os agentes, em determinados casos, de adotar dois conjuntos de cláusulas para uma mesma transferência de dados.

O procedimento poderá ser instaurado de ofício ou a requerimento dos interessados, acompanhado dos seguintes documentos e informações: inteiro teor das cláusulas-padrão contratuais, traduzidas para o português; legislação relevante aplicável ou qualquer documento pertinente, incluindo guias e orientações expedidos pela respectiva APD; e a análise de compatibilidade com as disposições da LGPD e da proposta de regulamento que inclua comparativo entre o conteúdo das cláusulas nacionais e das que se pretende obter reconhecimento de equivalência.[526]

A decisão sobre a proposta de equivalência levará em consideração, entre outras circunstâncias relevantes: se as cláusulas-padrão contratuais são compatíveis com as disposições da LGPD e regulamentos, bem como se asseguram nível de proteção de dados equivalente ao garantido pelas cláusulas-padrão contratuais nacionais; e os riscos e os benefícios proporcionados pela aprovação, considerando, entre outros aspectos, a garantia dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD, além dos impactos sobre o fluxo internacional de dados, relações diplomáticas e cooperação internacional do Brasil com outros países e organismos internacionais.

[526] Artigo 17, da proposta de regulamento de TIDP da ANPD.

A ANPD priorizará a aprovação de cláusulas que possam ser utilizadas em escala por outros agentes de tratamento que realizam transferências internacionais de dados em circunstâncias similares.[527]A decisão de equivalência deverá ser disponibilizada por meio de uma Resolução do Conselho Diretor no *website* da ANPD.[528]

3.3.4.5. Cláusulas Contratuais Específicas

Ainda nos termos da proposta de regulamento, em razão da singularidade de determinadas transferências internacionais de dados, o controlador poderá solicitar à ANPD a aprovação de cláusulas contratuais específicas, as quais somente serão aprovadas para transferências que não possam ser realizadas com base nas cláusulas-padrão contratuais, em função de circunstâncias excepcionais de fato ou de direito, devidamente comprovadas e justificadas pelo controlador.[529] As cláusulas contratuais específicas deverão prever a aplicação da legislação nacional de proteção de dados pessoais à transferência internacional de dados e a sua submissão à fiscalização da ANPD.[530]

De forma similar às cláusulas-padrão equivalentes, a aprovação pela ANPD das cláusulas específicas levará em consideração, entre outras circunstâncias relevantes: se as cláusulas específicas são compatíveis com as disposições da LGPD e regulamentos, bem como se asseguram nível de proteção de dados equivalente ao garantido pelas cláusulas-padrão contratuais nacionais; e os riscos e os benefícios proporcionados pela aprovação, considerando, entre outros aspectos a garantia dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD, além dos impactos quanto ao fluxo internacional de dados, relações diplomáticas e cooperação internacional do Brasil com outros países e organismos internacionais.[531]

3.3.4.6. Normas Corporativas Globais

As normas corporativas globais (NCG) são destinadas às transferências internacionais de dados pessoais entre organizações do mesmo grupo econômico, tendo caráter vinculante em relação a todos os membros do grupo. A proposta de regulamento define grupo ou conglomerado de empresas como o conjunto de empresas de fato ou de direito com personalidades jurídicas próprias, sob direção, controle ou administração de

[527] Artigo 18, da proposta de regulamento de TIDP da ANPD.
[528] Artigo 19, da proposta de regulamento de TIDP da ANPD.
[529] Artigo 20, art. 22, da proposta de regulamento de TIDP da ANPD.
[530] Artigo 20, §2º, da proposta de regulamento de TIDP da ANPD.
[531] Artigo 21, da proposta de regulamento de TIDP da ANPD.

uma pessoa natural ou jurídica ou ainda grupo de pessoas que detêm, isolada ou conjuntamente, poder de controle sobre a demais, desde que demonstrado interesse integrado, efetiva comunhão de interesses e atuação conjunta das empresas dele integrantes.[532]

Além disso, a proposta de regulamento inaugura a figura da entidade responsável, que constitui a sociedade empresária, com sede no Brasil, que responde por qualquer violação de norma corporativa global, ainda que decorrente de ato praticado por um membro do grupo econômico com sede em outro país.[533]As NCG deverão estar vinculadas ao estabelecimento e à implementação de programa de governança em privacidade, conforme os seguintes requisitos, no mínimo: [534]

> (1) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
> (2) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou a coleta;
> (3) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
> (4) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade e à proteção de dados pessoais;
> (5) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
> (6) esteja integrado à estrutura geral de governança, bem como estabeleça e aplique mecanismos de supervisão internos e externos;
> (7) conte com planos de resposta a incidentes e remediação; e
> (8) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Além de atender ao programa de governança em privacidade, as NCG deverão conter, no mínimo: [535]

> (1) especificação das categorias de transferências internacionais de dados para as quais o instrumento se aplica, incluindo as categorias de dados pessoais, a operação de tratamento e suas finalidades, a hipótese legal e os tipos de titulares de dados;
> (2) identificação dos países para os quais os dados são transferidos;
> (3) estrutura do grupo ou conglomerado de empresas, contendo a lista de entidades vinculadas, o papel exercido por cada uma delas no tratamento e os dados de contato de cada organização que efetue tratamento de dados pessoais;
> (4) determinação da natureza vinculante da norma corporativa global para todos os integrantes do grupo econômico, inclusive para seus funcionários;
> (5) delimitação de responsabilidades pelo tratamento, com a indicação da entidade responsável;
> (6) indicação dos direitos dos titulares aplicáveis e os meios para o seu exercício, incluindo canal de fácil acesso e o direito de peticionar contra o controlador perante a ANPD, após comprovada pelo titular a apresentação de

[532] Artigo 3º, VI, da proposta de regulamento de TIDP da ANPD.
[533] Artigo 3º, VII, da proposta deregulamento de TIDP da ANPD.
[534] Artigo 25, da proposta de regulamento de TIDP da ANPD.
[535] Artigo 26, da proposta de regulamento de TIDP da ANPD.

> reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;
> (7) regras sobre o processo de revisão das normas corporativas globais e previsão de submissão à prévia aprovação da ANPD; e
> (8) previsão de comunicação à ANPD em caso de alterações nas garantias apresentadas como suficientes de observância dos princípios, dos direitos do titular e do regime de proteção de dados previsto na LGPD, especialmente na hipótese em que um dos membros do grupo estiver submetido à determinação legal de outro país que impeça o cumprimento das normas corporativas. Nesse último caso, deverá ser igualmente prevista a obrigação de notificação imediata à entidade responsável, ressalvada a hipótese de expressa proibição legal de realizar essa notificação.

3.3.4.7. O processo de aprovação de Cláusulas Contratuais Específicas e de Normas Corporativas Globais

As cláusulas contratuais específicas e as NCG deverão ser aprovadas pela ANPD, como prevê proposta de regulamento. Com relação ao requerimento de aprovação, o documento deverá ser instruído com a minuta de contrato ou da norma corporativa, os documentos de constituição social do agente de tratamento ou grupo econômico e a demonstração do atendimento aos requisitos de cada uma das modalidades. Poderá ser requerida a apresentação de outros documentos e informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.[536] O requerimento de aprovação de cláusulas contratuais específicas e de NCG será analisado pela área técnica competente da ANPD, que se manifestará sobre o mérito do pedido, indicando, se for o caso, as condicionantes a serem observadas.[537]As alterações nas cláusulas contratuais específicas e nas NCG dependem de prévia aprovação da ANPD.[538]

3.3.4.8. Exceções previstas na legislação brasileira de proteção de dados

O artigo 33 refere-se também às exceções que justificam a realização da transferência internacional de dados pessoais. Elas incluem a transferência necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, investigação e persecução, de acordo com os instrumentos de Direito Internacional. Também se aplica quando a transferência for essencial para proteger a vida ou integridade física do titular dos dados ou de terceiros. Além disso, a ANPD pode autorizar a

[536] Artigo 28, da proposta de regulamento de TIDP da ANPD.
[537] Artigo 29, da proposta de regulamento de TIDP da ANPD.
[538] Artigo 33, da proposta de regulamento de TIDP da ANPD.

transferência, ou esta pode resultar em um compromisso em acordo de cooperação internacional.

A transferência também é permitida quando necessária para a execução de política pública ou atribuição legal do serviço público, ou quando o titular dos dados consentir, especificamente e em destaque para tal, com informação prévia sobre o caráter internacional da operação. Por fim, é justificável quando necessário para cumprir obrigações legais ou regulatórias pelo controlador, para execução de contrato ou procedimentos preliminares relacionados a contrato do qual o titular dos dados seja parte, a pedido deste, e para o exercício regular de direitos em processos judiciais, administrativos ou arbitrais.

3.4. Aspectos relevantes do tema em perspectiva comparada

A partir da análise dos regimes de tutela das transferências internacionais de dados pessoais do Brasil, da Argentina, do Uruguai e da Colômbia, observa-se que diversas disposições relativas à matéria, previstas nas leis de proteção de dados abordadas, devem ser preenchidas pela atuação das APD. Uma questão que se destaca é que, apesar de a legislação de proteção de dados da Argentina estar em vigor há anos, apenas recentemente a sua APD emitiu regulamentos para definir determinados mecanismos de transferências. Na Colômbia e no Uruguai esse movimento também se intensificou nos últimos anos. No Brasil, embora a versão definitiva do Regulamento da ANPD sobre o tema ainda esteja pendente de publicação até a data de conclusão desta pesquisa, a proposta que foi examinada traça as bases que serão implementadas no país e constitui instrumento relevante para este estudo. Percebe-se, assim, um empenho na criação e atualizações de regulamentos relacionados aos mecanismos de transferências internacionais de dados pessoais por todas as APD abordadas recentemente.

Em todos os regimes analisados, é evidente a exigência de que o país destinatário dos dados tenha nível adequado de proteção para que a transferência internacional de dados pessoais seja autorizada, o que reflete a difusão do requisito de adequação da UE na região latino-americana. Nota-se que os critérios de avaliação do nível de proteção estabelecidos em cada país buscam incorporar elementos que vão além da comparação de textos legais e, em geral, incluem parâmetros como a existência de mecanismos de proteção disponíveis ao titular para proteger seus dados e de autoridades de supervisão para efetivar essa proteção. Contudo, para determinar as circunstâncias concretas do país avaliado, cabe ponderar que é necessário que as APD sejam capazes de

avaliar a eficácia desses mecanismos e a estrutura das autoridades no país destinatário dos dados, incluindo, entre outros aspectos, o seu grau de independência e a sua capacidade de atuação. Com isso, seria possível avaliar o nível de proteção real em relação às práticas do país.

Outro ponto que merece atenção presente nos critérios de avaliação do nível de proteção é a abordagem adotada, sobretudo pelo Uruguai, que pressupõe que os países que já foram objeto de decisão de adequação pelas entidades europeias oferecem proteção adequada. Ao sugerir uma confiança significativa nas avaliações europeias, essa abordagem dispensa que sejam realizadas as suas próprias avaliações em contextos específicos e acarreta um desafio adicional quando há alteração do status de adequação de um país pela UE, como ocorreu com a invalidação do *Privacy Shield* pelo TJUE.

Entre a Argentina e o Uruguai, há um reconhecimento recíproco de um nível adequado de proteção. Paralelamente, a Colômbia reconhece tanto a Argentina quanto o Uruguai, inclusive pelo fato de ambos terem sido considerados países com nível de proteção adequado pela Comissão Europeia. No entanto, é importante mencionar que nem a Argentina, nem o Uruguai reconheceram a Colômbia, até o momento. O Brasil, devido à implementação recente da LGPD, ainda não foi reconhecido, nem estendeu reconhecimento a nenhum dos países abordados. Cabe acompanhar como esse quadro irá se desenvolver e, mais especificamente no âmbito do comércio eletrônico, se o Acordo do Mercosul servirá de estímulo para decisões de adequação.

Contudo, diante da existência de nuances nos critérios de avaliação do nível de proteção, ainda que um país seja avaliado como adequado sob uma perspectiva, pode não ser reconhecido ou até considerado inadequado sob outra. A Colômbia, por exemplo, foi o único país abordado a reconhecer a adequação dos EUA. No Brasil, por sua vez, a proposta de regulamento da ANPD reservou espaço para que a decisão de adequação considere não apenas um exercício jurídico, mas também um balanço de questões estratégicas e diplomáticas. Com efeito, observa-se que a avaliação do nível de proteção envolve critérios diversos e pode representar um processo complexo, incluindo fatores políticos e econômicos. Isso pode acarretar dificuldades para a uniformidade das decisões de adequação.

Além dessa solução, todos os regimes analisados estabelecem mecanismos voluntários que autorizam as transferências internacionais de dados pessoais. Os regulamentos emitidos pelas APD nos últimos anos dizem respeito, sobretudo, às cláusulas-padrão contratuais e às normas corporativas vinculantes ou globais. Isso

também reflete uma tendência para acompanhar as atualizações europeias. Mesmo diante de uma decisão de adequação, observa-se que no Uruguai e na Colômbia, as suas respectivas APD incentivam o uso de tais mecanismos de forma complementar para disciplinar a relação dos agentes envolvidos na transferência, possibilitando a alocação de obrigações e responsabilidades entre os exportadores e importadores, considerando suas características e as operações desenvolvidas.

Os instrumentos contratuais e as cláusulas-padrão contratuais analisados são, em geral, adaptáveis, variando conforme o papel do exportador ou importador, seja como controlador dos dados, seja como operador dos dados. Enquanto alguns países traçam diretrizes para a formulação dessas cláusulas, como o Uruguai e a Colômbia, outros especificam sua redação, como a Argentina e o Brasil. Existem abordagens diferentes quanto à intervenção das APD, que podem exigir a aprovação antes da implementação dos instrumentos contratuais, especialmente quando o agente não aderir ao modelo padrão pré-aprovado pela autoridade correspondente e/ou a sua supervisão após já estarem em vigor. Ressalta-se a tendência de que as diretrizes e cláusulas-padrão contratuais estabelecem condições específicas para o caso de autoridades públicas estrangeiras requisitarem acesso a dados pessoais, incluindo o envio de notificação para o exportador. Dessa forma, o importador deve observar salvaguardas disciplinadas contratualmente na ocorrência de pedidos de acesso a dados por autoridades públicas.

Ainda, a Argentina e o Uruguai admitiram as cláusulas contatuais modelo da RIPD como mecanismos válidos. É possível que a Colômbia e o Brasil adotem uma postura semelhante. Esse movimento pode representar a convergência de mecanismos entre os países e simplificar procedimentos para os fluxos entre eles, desonerando os agentes de adotar dois conjuntos de cláusulas para uma mesma transferência. Notavelmente, no Brasil, a proposta de regulamento da ANPD permite reconhecer cláusulas-padrão contratuais equivalentes que são provenientes de outros países ou organismos. Com a recente divulgação das cláusulas contatuais modelo do Conselho da Europa, também espera-se o posicionamento das autoridades da Argentina e do Uruguai com relação à sua incorporação, uma vez que ambos são Estados-partes da Convenção 108+.

Adicionalmente, observa-se que os regulamentos emitidos pelas APD sob análise, em geral, descrevem diretrizes e requisitos mínimos para a elaboração de normas corporativas vinculantes ou globais e, em alguns casos, códigos de conduta. Além de admitirem a autorregulação, os referidos regulamentos requerem o controle desses

mecanismos pelas APD, que são responsáveis pela sua validação e/ou supervisão. Em contraste, o uso de selos de certificação como mecanismos de transferências internacionais de dados nos regimes abordados carece de maior clareza na região. Com a evolução do Fórum Global CBPR, é importante acompanhar como os países abordados irão se posicionar, uma vez que o reconhecimento da certificação CBPR pode estabelecer um novo mecanismo, afetando o modo como as transferências internacionais de dados pessoais são realizadas na região.

Nos regimes analisados, o uso dos mecanismos voluntários acima descritos também requer a implementação de medidas com base na responsabilidade dos agentes, tendo como referência os denominados princípios de "responsabilidade demonstrada", "responsabilidade proativa" e de "prestação de contas" (*accountability*). A inclusão de medidas responsáveis como parte dos instrumentos regulatórias tem destaque e demonstra um esforço para que os exportadores assegurem que os importadores irão tratar os dados transferidos de forma consistente com os padrões do país de origem. De igual modo, o dimensionamento dos riscos associados às transferências é um requisito amplamente adotado pelos regimes analisados e está frequentemente ligado à responsabilidade dos agentes. Essa avaliação pode envolver o exame de leis e práticas do país destinatário que acarretem risco para o cumprimento das obrigações assumidas nas transferências.

Ressalta-se que o trabalho colaborativo das APD da Argentina e do Uruguai no *Guia de Evaluación de Impacto en la Protección de Dato* apresenta critérios para a avaliação de riscos e evidencia um movimento regional para estabelecer padrões comuns em matéria de proteção de dados. O *Guía para la Implementación del Principio de Responsabilidad Demostrada en las Transferencias Internacionales de Datos Personales* da SIC também fornece parâmetros e pode servir como uma referência para a aplicação dos princípios de responsabilidade e prestação de contas. Em tais documentos, observa-se que foi dedicada atenção particular à implementação de medidas de segurança, inclusive de natureza técnica e por padrão (*privacy by design and by default*), para proteger os dados transferidos de forma proporcional ao grau de risco identificado.

Além dos mecanismos voluntários, os regimes dos países abordados estabelecem um conjunto de derrogações, em geral, similares para as transferências internacionais de dados, que são aplicadas em situações específicas, muitas vezes, em razão de necessidades imediatas, como por razões de saúde e proteção da vida do titular. O consentimento está presente em todas as exceções dos regimes analisados. Contudo, convém ponderar que, em situações de transferências internacionais de dados pessoais

regulares, o consentimento atribui peso significativo sobre o titular dos dados, de modo que é importante que sejam implementadas práticas responsáveis pelos agentes envolvidos para garantir transferências seguras. Como resultado da análise, os Quadros a seguir foram elaborados para apresentar, de forma sistematizada, os regimes de tutela das transferências internacionais de dados pessoais em cada um dos países abordados.

Quadro 2 – Análise sistematizada dos regimes de tutela das transferências internacionais de dados da Argentina

	Regime	**Normativa**
Argentina	Nível adequado de proteção de dados do país terceiro	• Lei nº 25.326/2000 • Decreto nº 1558/2001 • Resolución nº 34/2019 da AAIP
	Nível adequado de proteção decorrente de salvaguarda proporcionada por instrumentos contratuais: cláusulas-padrão contratuais	• Lei nº 25.326/2000 • Decreto nº 1558/2001 • *Disposición* nº 60/2016 da AAIP • *Guia de Evaluación de Impacto en la Protección de Datos* da AAIP e da URCDP • *Resolución* nº 198/2023
	Nível adequado de proteção decorrente de sistemas de autorregulação: Normas Corporativas Vinculantes	• Lei nº 25.326/2000 • Decreto nº 1558/2001 • *Resolución* nº 159/2018 da AAIP (Anexo I).
	Exceções previstas na legislação	• Lei nº 25.326/2000 • Decreto nº 1558/2001

Quadro 3 – Análise sistematizada dos regimes de tutela das transferências internacionais de dados do Uruguai

	Regime	**Normativa**
Uruguai	Nível adequado de proteção de dados do país terceiro	• Lei nº 18.331/2008 • Decreto n° 414/009 • *Resolución* nº 23/2021 da URCDP
	Autorização da URCDP: cláusulas contratuais apropriadas e códigos de conduta	• Lei nº 18.331/2008 • Decreto n° 414/009 • Lei nº 19.670/2018 • Decreto nº 64/2020 • *Resolución* nº 41/2021 da URCDP • *Guia de Evaluación de Impacto en la Protección de Datos* da AAIP e da URCDP • *Resolución* n° 50/022
	Exceções previstas na legislação	• Lei nº 18.331/2008 • Decreto n° 414/009

Quadro 4 – Análise sistematizada dos regimes de tutela das transferências internacionais de dados da Colômbia

	Regime	Normativa
Colômbia	Nível adequado de proteção de dados do país terceiro	• Lei nº 1.581/2012 • Decreto nº 1377/ 2013 • Título V da Circular Única da SIC • *Guía para la Implementación del Principio de Responsabilidad Demostrada* da SIC • *Guía para la Implementación del Principio de Responsabilidad Demostrada en las Transferencias Internacionales de Datos Personales* da SIC
	Normas Corporativas Vinculantes	• Lei nº 1.581/2012 • Decreto nº 1.377/2013 • Decreto nº 255/2022
	Exceções previstas na legislação	• Lei nº 1.581/2012 • Decreto nº 1.377/2013
	Decisão de Conformidade da SIC e Contrato de Transferência Internacional de Dados	• Lei nº 1.581/2012 • Decreto nº 1.377/2013 • Título V da Circular Única da SIC • *Guía para Solicitar la Declaración de Conformidad sobre las Transferencias Internacionales de Datos Personales* da SIC • *Guía para la Implementación del Principio de Responsabilidad Demostrada en las Transferencias Internacionales de Datos Personales* da SIC
	Contrato de Transmissão de Dados	• Lei nº 1.581/2012 • Decreto nº 1.377/2013 • Título V da Circular Única da SIC

Quadro 5 – Análise sistematizada dos regimes de tutela das transferências internacionais de dados do Brasil

	Regime	Normativa
Brasil	Nível adequado de proteção de dados do país terceiro	• LGPD • Proposta de regulamento de Transferência Internacional de Dados da ANPD
	Garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD na forma de: cláusulas-padrão contratuais, cláusulas-padrão contratuais equivalentes, cláusulas contratuais específicas, normas corporativas globais.	• LGPD • Proposta de regulamento de Transferência Internacional de Dados da ANPD e Anexo II
	Selos, Certificados e Códigos de Conduta	• LGPD
	Exceções previstas na legislação	• LGPD

Fonte: elaboração própria

3.5. Conclusão do Capítulo

Com base nas definições exploradas neste Capítulo, as transferências internacionais de dados ocorrem quando um agente, o exportador, envia dados pessoais de um país para outro agente, o importador, que está localizado em um país distinto. Essa operação se distingue da coleta internacional de dados, na qual um agente situado no exterior obtém diretamente dados pessoais do titular. Nas transferências internacionais, é requerida a implementação de mecanismos para assegurar a continuidade da proteção dos dados no país destinatário, já nas coletas internacionais os dados pessoais frequentemente estão sob os efeitos extraterritoriais das leis de proteção de dados sob análise.

O cotejo entre os regimes de tutela das transferências internacionais de dados pessoais analisados neste Capítulo conduz à conclusão de que os mecanismos voluntários oferecem meios para promover as transferências de dados pessoais entre o Brasil, a Argentina, o Uruguai e a Colômbia. Isso decorre do enfoque atribuído à avaliação de riscos e às medidas de responsabilização e prestação de contas (*accountability*) por meio das quais os agentes deverão comprovar garantias substantivas de proteções aos dados pessoais transferidos que foram assumidas, sobretudo, contratualmente ou em regras corporativas vinculantes ou globais. Nos regimes analisados, os mecanismos voluntários representam meios para possibilitar a adesão de padrões de proteção de dados de sistemas jurídicos distintos.

O estabelecimento de práticas responsáveis e a identificação dos impactos associados às transferências internacionais permitem a implementação de medidas pelos agentes que se moldam a diferentes contextos e que podem ser adaptadas a novos desenvolvimentos tecnológicos. Para um cenário mais integrado entre os países abordados, seria oportuno que, de forma conjunta, as APD apresentassem orientações e padrões comuns sobre como as medidas de responsabilização e prestação de contas são aplicáveis aos mecanismos voluntários para assegurar transferência confiáveis e seguras na região, na linha do que foi feito pela AAIP e pela URCPD com o *Guia de Evaluación de Impacto en la Protección de Datos.*

Ainda, percebe-se que a regulamentação dos mecanismos voluntários no cenário mais recente decorre de uma necessidade de expandir as condições legais que autorizam as transferências de dados para além das fronteiras, com o intuito de oferecer vias adaptáveis e dinâmicas para atender às exigências legais, sem prejudicar a eficiência e dinamicidade dos negócios. Os agentes envolvidos nas transferências podem aderir a

esses mecanismos e, em geral, as APD correspondentes devem aprová-los e/ou supervisionar seu cumprimento, o que reflete o caráter híbrido associado a essa estratégia regulatória.

Não obstante, a supervisão dos mecanismos voluntários não está isenta de desafios. O processo de responsabilização dos agentes em situações de violação pode requerer atuações coordenadas das APD nas diferentes jurisdições. Ainda, a aprovação de tais mecanismos e a fiscalização contínua por parte das APD exige recursos suficientes, tanto financeiros quanto humanos e de expertise técnica, para gerir um volume substancial de transferências internacionais. Isso é evidente no contexto de instrumentos contratuais e de normas corporativas vinculantes ou globais que requerem a aprovação, pelas autoridades, correspondentes antes de serem implementados. Assim, é indispensável que as APD tenham uma estrutura independente, robusta e meios de cooperação eficientes.

A esse respeito, a intensificação da cooperação entre as APD poderá contribuir para a supervisão dos mecanismos nas transferências internacionais de dados pessoais. Para tanto, o fortalecimento de espaços de diálogo e de acordos entre as APD se colocam como possíveis caminhos. Como explorado nesta pesquisa, a RIDP pode servir como local para a troca regular de informações, incluindo sobre atualizações das respectivas leis de proteção de dados, compartilhamento de melhores práticas e de expertise técnica e planejamento de ações conjuntas. Assim, a RIPD pode proporcionar um ambiente para nutrir a cooperação entre as APD, possibilitando debates que exploram desafios e soluções comuns, incluindo a participação do setor privado e da sociedade civil.

CONCLUSÃO

A temática das transferências internacionais de dados pessoais está, indiscutivelmente, em rápida evolução. Ao longo do desenvolvimento desta pesquisa, novas normativas no assunto foram aprovadas e outras vêm sendo debatidas, refletindo respostas aos desafios apresentados pela era digital. Isso não apenas evidencia a relevância dos fluxos de dados entre países na atualidade, mas também a sua relação com as transformações econômicas, políticas e sociais. O ritmo acelerado reforça a necessidade de uma análise contínua do tema, garantindo que os regimes de tutela das transferências internacionais sejam eficazes.

Como analisado nesta pesquisa, as discussões regulatórias sobre transferências internacionais de dados enfrentam questões complexas, como a existência de diferentes leis de proteção de dados ao redor do mundo e a potencial exploração dessas diferenças pelos agentes. Esta pesquisa centrou-se na análise dos regimes de tutela das transferências internacionais de dados pessoais do Brasil, da Argentina, do Uruguai e da Colômbia, buscando compreender os seus impactos para fluxos de dados seguros e confiáveis entre os países. Constatou-se que a definição de mecanismos e procedimentos interoperáveis é importante para a segurança jurídica, bem como para fortalecer as proteções asseguradas aos titulares dos dados.

A crescente relevância dos dados pessoais em várias esferas motivou o tratamento autônomo da proteção de dados pelos ordenamentos jurídicos de diversos países, de forma distinta da privacidade. Devido às inovações trazidas pelas TIC, especialmente a computação em nuvem e a IoT, hoje é possível realizar transferências internacionais de dados pessoais de maneira regular e dinâmica. Nesse contexto, a Internet, descrita como a "rede das redes", emerge como a principal via para a transposição desses dados por sobre as fronteiras.

A partir das contribuições das teorias de regulação da Internet, pode-se observar que os regimes para a tutela das transferências internacionais de dados pessoais podem alcançar maior interoperabilidade com base em modelos regulatórios híbridos. Esses modelos distribuem responsabilidades entre os diversos atores envolvidos no processo regulatório e podem incluir instrumento e estratégias que contemplem a proteção de dados na arquitetura, a responsabilização e prestação de contas (*accountability*) dos agentes, além de avaliações para dimensionar os riscos associados às transferências.

Como era de se esperar, as transferências de dados pessoais entre países, desde a década de 1970, motivaram iniciativas internacionais e regionais para a troca de conceitos e práticas de proteção de dados, com organizações como OCDE e o Conselho da Europa desempenhando papéis de liderança. Instrumentos resultantes desse movimento, sobretudo as Diretrizes de Privacidade da OCDE e as Convenções 108 e 108+ do Conselho da Europa, têm sido relevantes para a consolidação de padrões comuns no tema. Essa tendência se estendeu para fóruns em outras regiões, abrangendo a atuação expressiva da APEC e da RIPD e, recentemente, do Mercosul no contexto do comércio eletrônico.

Constata-se um esforço desse movimento para reduzir barreiras injustificadas que possam impedir o fluxo de dados entre os países que estejam alinhados com os instrumentos internacionais e regionais dessas organizações. Para isso, verifica-se que foram adotadas abordagens híbridas, que incluem mecanismos voluntários como cláusulas contratuais e meios de autorregulação vinculante que ofereçam garantias suficientes de proteção. O sistema de certificação do Fórum Global CBPR se destaca por seu potencial de promover, globalmente, padrões de proteção de dados e de trazer um novo cenário para os fluxos de dados entre países.

Nesse sentido, observa-se que inciativas isoladas para regular a proteção de dados possuem eficácia limitada, conduzindo a uma busca pela interconexão entre as distintas construções jurídicas no tema. Isso é particularmente evidente no conflito travado ao longo dos anos entre a UE e os EUA. A despeito das diferenças nos seus modelos regulatórios de proteção de dados, uma conclusão que se extrai desta pesquisa é que a abordagem norte-americana aparenta estar se movendo em direção aos padrões europeus de proteção de dados. A Ordem Executiva do Presidente Biden, que foca no Desenvolvimento Seguro, Protegido e Confiável da Inteligência Artificial, indica ao Congresso a necessidade de avançar na aprovação de uma legislação federal de privacidade.

O mesmo se observa no âmbito do *Data Privacy Framework* entre UE e EUA, notadamente, com a implementação da Ordem Executiva para o Fortalecimento das Proteções das Atividades de Inteligência de Sinais, que estabelece garantias para limitar o acesso a dados pessoais pelas autoridades públicas norte-americanas ao que é necessário e proporcional nas atividades de segurança, além de instituir mecanismos institucionais para endereçar reclamações nesse tema. Essa última Ordem Executiva inova também na sua abrangência e no princípio de reciprocidade.

Com efeito, as tensões marcadas entre a UE e os EUA sublinharam um problema reiterado para a tutela das transferências internacionais de dados pessoais, que se traduz nas situações em que o setor público busca acessar dados pessoais, a partir do setor privado, para desempenhar atividades de segurança. Esse cenário, portanto, remete a outra conclusão desta pesquisa, que se refere à necessidade de estabelecer balizas para uma proteção integral de dados, envolvendo contextos de atividades de segurança e persecução penal. Uma agenda para a proteção de dados que destaca essa temática também deve ser objeto de reflexão pelos países latino-americanos frente aos desafios atuais e para avançar na promoção de transferências internacionais de dados pessoais seguras e confiáveis na região.

No decorrer do tempo, a trajetória da proteção de dados na América Latina foi moldada por motivações históricas, econômicas e sociais, juntamente com a evolução tecnológica e as pressões globais para regulação do tema. O *Habeas Data*, instrumento processual distintivo da região, demonstra variações de abrangência e de eficácia entre os países abordados. Apesar de inicialmente alguns países terem se alinhado ao modelo norte-americano, devido à interpretação judicial pela ação de *Habeas Data*, nota-se que a influência europeia prevaleceu, especialmente com o reconhecimento da proteção de dados como um direito fundamental.

Nos últimos 20 anos, o Brasil, a Argentina, o Uruguai e a Colômbia consolidaram esse direito, incorporando disposições constitucionais e promulgando leis gerais sobre o tema, além de instaurar APD para sua supervisão. Verifica-se a adesão de certos países abordados a tratados internacionais de proteção de dados, como as Convenções 108 e 108+ e a Convenção de Budapeste do Conselho da Europa. Paralelamente, observa-se o fortalecimento regional na questão da proteção de dados, com a atuação da RIDP.

Com base nas definições das leis e regulamentos de proteção do Brasil, da Argentina, do Uruguai e da Colômbia, identifica-se o conceito jurídico de transferências internacionais de dados pessoais, que ocorrem quando um agente, o exportador, envia dados pessoais de um país para outro agente, o importador, que está localizado em um país distinto. A compreensão adequada deste conceito requer a sua diferenciação da coleta internacional de dados pessoais, que acontece quando os dados são obtidos diretamente dos titulares por um agente situado no exterior. A partir da análise dos regimes de tutela das transferências internacionais de dados pessoais, constata-se que, a despeito da difusão do requisito de adequação da UE na região, que exige que o país destinatário dos dados

tenha nível adequado de proteção para autorizar a transferência internacional, a avaliação desse nível pode envolver critérios diversos e representar um processo complexo, incluindo fatores políticos e econômicos. As limitações dessa solução no âmbito da UE também foram identificadas nesta pesquisa.

Portanto, à luz do problema de pesquisa posto, a conclusão decorrente da análise dos regimes é que os mecanismos voluntários configuram-se instrumentos para promover as transferência de dados entre Brasil, Argentina, Uruguai e Colômbia. Isso porque as leis e regulamentos de proteção de dados analisados requerem que tais mecanismos sejam associados à avaliação de riscos e à implementação de medidas de responsabilização e prestação de contas (*accountability*). Os agentes envolvidos na transferência devem demonstrar garantias substantiva de proteção aos dados pessoais assumidas, sobretudo, por meio de contratos e regras corporativas vinculantes ou globais.

Estabelecer práticas responsáveis e avaliar os impactos permite que os agentes desenvolvam medidas adaptáveis a diferentes contextos nas transferências internacionais, bem como em tecnologias emergentes. Nesse sentido, seria oportuno que as APD desses países trabalhassem de forma conjunta para fornecer orientações e padrões comuns sobre como aplicar medidas de responsabilização e prestação de contas nos mecanismos voluntários, de modo a promover transferências de dados pessoais seguras e confiáveis na região.

Para lidar com os desafios associados à supervisão de tais mecanismos, a intensificação da cooperação direta e de acordos entre as APD se colocam como possíveis caminhos. Isso poderá envolver o fortalecimento de espaços de diálogo, como a RIPD, para a troca regular de informações sobre proteção de dados, incluindo atualizações legislativas, compartilhamento de melhores práticas e planejamento de ações conjuntas. A RIPD também pode facilitar debates envolvendo o setor privado e a sociedade civil, focando em desafios e soluções comuns na proteção de dados pessoais.

REFERÊNCIAS

AAIP - AGENCIA DE ACCESO A LA INFORMACIÓN PUBLICA. Disposición nº 60/2016. **Clausulas Contractuales Tipo de Transferencia Internacional - Aprobacion**. 16 nov. 2016. Disponível em: https://www.argentina.gob.ar/normativa/nacional/267922/texto. Acesso em: 2 nov. 2023.

_____. Ley de protección de los datos personales en Argentina: **sugerencias y aportes recibidos en lo proceso de reflexión sobre la necesidad de su reforma**, ago. 2017. Disponível em: https://www.argentina.gob.ar/sites/default/files/documento_aportes_reforma_ley25326_0.pdf. Acesso em: 2 nov. 2023.

_____. Resolución nº 159/2018: **Lineamientos y Contenidos Basicos de Normas Corporativas Vinculantes**. 5 dez. 2018. Disponível em: https://www.boletinoficial.gob.ar/detalleAviso/primera/197428/20181207. Acesso em: 2 nov. 2023.

_____. Resolución nº 34/2019: **Disposicion 60 - E/2016 - Modificacion**. 22 fev. 2019 Disponível em https://www.boletinoficial.gob.ar/detalleAviso/primera/202373/20190226. Acesso em: 2 nov. 2023.

_____. **Informe sobre el proceso de Elaboración Participativa de Normas en relación al anteproyecto de Ley de Protección de Datos Personales**, out. 2022. Disponível em:https://www.argentina.gob.ar/sites/default/files/informe_consulta_publica_aaip_pdf. Acesso em: 2 nov. 2023.

_____. **Presentación del Proyecto de Ley de Protección de Datos Personales**, nov. 2022(b). Disponível em: https://www.argentina.gob.ar/noticias/presentacion-del-proyecto-de-ley-de-proteccion-de-datos-personales. Acesso em: 2 nov. 2023.

_____. **Proyecto de Ley de Protección de Datos Personales**, out. 2022(c). p. 45. Disponível em: https://www.argentina.gob.ar/sites/default/files/proyecto_de_ley_de_datos_personales_aaip.pdf. Acesso em: 2 nov. 2023.

_____. **Registro de Bases de Datos Personales para responsables extranjeros.** 29 nov. 2022(d). Disponível em: https://www.argentina.gob.ar/noticias/registro-de-bases-de-datos-personales-para-responsables-extranjeros. Acesso em: 2 nov. 2023.

_____. **Normativa**. 2023. Disponível em: https://www.argentina.gob.ar/aaip/buscador-normativa. Acesso em: 2 nov. 2023.

_____. **Obligaciones de los responsables de bases de datos personales**. 2023(b). Disponível em: https://www.argentina.gob.ar/aaip/datospersonales/responsables/obligaciones. Acesso em: 2 nov. 2023.

_____. **La titular de la AAIP depositó en representación de la Argentina el instrumento de ratificación del convenio 108+**. 18 mar. 2023(c). Disponível em:

https://www.argentina.gob.ar/noticias/la-titular-de-la-aaip-deposito-en-representacion-de-la-argentina-el-instrumento-de. Acesso em: 2 nov. 2023.

_____. Resolución 94/2023**: Plan Estrategico 2022-2026**. 23 mai. 2023(d). Disponível em: https://www.boletinoficial.gob.ar/detalleAviso/primera/287117/20230524. Acesso em: 2 nov. 2023.

_____. Resolución nº 198/2023: **Modelo Para Transferencias Internacionales - Clausulas Contractuales**. 18 out. 2023(e). Disponível em: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-198-2023-391538. Acesso em: 2 nov. 2023.

AAIP; URCDP. **Guía de Evaluación de Impacto en la Protección de Datos**. 28 jan. 2020. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-evaluacion-impacto-proteccion-datos. Acesso em: 2 nov. 2023.

ALHADEFF, Joseph; VAN ALSENOY, Brendan; DUMORTIER, Jos. The accountability principle in data protection regulation: origin, development and future directions. In: **Managing privacy through accountability**. London: Palgrave Macmillan UK, 2012. pp. 49-82.

ANPD - AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **ANPD torna-se membro da Rede Ibero-Americana de proteção de dados**. 21 out. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-torna-se-membro-da-rede-ibero-americana-de-protecao-de-dados. Acesso em: 2 nov. 2023.

_____. **ANPD participa da 43ª Reunião Plenária da Convenção 108, na França**. 17 nov. 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-participa-da-43a-reuniao-plenaria-da-convencao-108-na-franca. Acesso em: 2 nov. 2023.

_____. **Tomada de Subsídios sobre Transferência Internacional**. 2022(b). Disponível em: https://www.gov.br/participamaisbrasil/tomada-de-subsidios-transferencia-internacional. Acesso em: 2 nov. 2023.

_____. **Regulamento de Transferências Internacionais de Dados Pessoais.** 2023. Disponível em: https://www.gov.br/participamaisbrasil/regulamento-de-transferencias-internacionais-de-dados-pessoais-e-do-modelo-de-clausulas-padrao-contratuais. Acesso em: 2 nov. 2023.

_____. **Aberta Consulta Pública sobre norma de transferências internacionais de dados pessoais**. 15 ago. 2023(b). Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/aberta-consulta-publica-sobre-norma-de-transferencias-internacionais-de-dados-pessoais. Acesso em: 2 nov. 2023.

_____. **ANPD representa o Brasil na 44ª Reunião Plenária do Comitê Consultivo da Convenção 108.** 15 jun. 2023(c). Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-representa-o-brasil-na-44a-reuniao-plenaria-do-comite-consultivo-da-convencao-108. Acesso em: 2 nov. 2023.

ASOCIACIÓN POR LOS DERECHOS CIVILES - ADC. **El Sistema de Protección de Datos Personales en América Latina**. Ciudad de Buenos Aires, 30 dez. 2016. E-book.

Disponível em: https://adc.org.ar/informes/sistema-proteccion-datos-personales-latam/. Acesso em: 2 nov. 2023.

APEC – ASIA-PACIFIC ECONOMIC COOPERATION. APEC. **APEC Privacy Framework**. Asia-Pacific Economic Cooperation. dez. 2005. Disponível em: https://www.apec.org/publications/2005/12/apec-privacy-framework. Acesso em: 2 nov. 2023.

_____. **APEC Cross-Border Privacy Rules System Policies, Rules and Guidelines.** 2011. Disponível em: http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_desarrollos_APEC_3.pdf. Acesso em: 2 nov. 2023.

_____. **APEC Privacy Recognition for Processors ("PRP") Purpose and Background**. 28 ago. 2015. Disponível em: http://cbprs.org/wp-content/uploads/2020/08/PRP-Purpose-and-Background-4.pdf. Acesso em: 2 nov. 2023.

_____. **APEC Privacy Framework.** Asia-Pacific Economic Cooperation, 2015. Disponível em: https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015). Acesso em: 2 nov. 2023.

_____. **About APEC: History**, out. 2023. Disponível em: https://www.apec.org/about-us/about-apec/history. Acesso em: 2 nov. 2023.

_____. **APEC Cross-Border Privacy Rules (CBPR) System**. 2023(b). Disponível em: https://cbprs.org. Acesso em: 2 nov. 2023.

_____. **What is the Cross-Border Privacy Rules System**, jun. 2023(c). Disponível em: https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system#:~:text=The%20APEC%20Cross%2DBorder%20Privacy,internationally%2Drecognized%20data%20privacy%20protections. Acesso em: 2 nov. 2023.

ARANHA, Mário Iório. Diálogo político-jurídico na comparação de modelos regulatórios de comunicação. **Revista Brasileira de Políticas de Comunicação**, v.1, 2011. pp. 1-20.

ARANHA, Marcio Iorio; LOPES, Othon. **Estudo sobre Teorias Jurídicas da Regulação apoiadas em incentivos**. Pesquisa e Inovação Acadêmica sobre Regulação apoiada em Incentivos na Fiscalização Regulatória de Telecomunicações, ANATEL/UnB, 2019.

ARGENTINA. **Constitución de la Nación Argentina**, 1994. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm. Acesso em: 2 nov. 2023.

_____. Corte Suprema de Justicia de la Nación**, Urteaga, Facundo Raúl c/ Estado Nacional – Estado Mayor Conjunto de las FF.AA. – s/amparo Ley 16.986**. Buenos Aires: 1998. Disponível em: http://www.saij.gob.ar/corte-suprema-justicia-nacion-federal-ciudad-autonoma-buenos-aires-urteaga-facundo-raul-estado-nacional-estado-mayor-conjunto-ffaa-amparo-ley-16986-fa98001242-1998-10-15/123456789-242-1008-9ots-eupmocsollaf. Acesso em: 2 nov. 2023.

_____. Lei nº 25.326, de 30 de outubro de 2000. Ley de Protección de Datos Personales. **Boletín Oficial:** Buenos Aires, ano 2000, n. 29517, p. p. 2 nov. 2000. p. 1. Disponível em: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/actualizacion. Acesso em: Acesso em: 2 nov. 2023.

_____. Decreto nº 1558/2001**. Apruébase la reglamentación de la Ley nº 25.326**. 2001. Disponível em: https://www.argentina.gob.ar/normativa/nacional/decreto-1558-2001-70368/actualizacion. Acesso em: 2 nov. 2023.

_____. Ley 27.275/2016. **Derecho de Acesso a la Información Pública.** Honorable Congreso de la Nacion Argentina, 6 set. 2016. Disponível em: https://www.argentina.gob.ar/normativa/nacional/ley-27275-265949/actualizacion. Acesso em: 2 nov. 2023.

BARLOW, John Perry. **Declaration of independence for cyberspace**. 1996. Disponível: https://www.eff.org/cyberspace-independence. Acesso em: 2 nov. 2023.

BASTERRA, Marcela. **Protección de datos personales: la garantia de habeas data**. Buenos Aires: Ediar, 2008.

BASTERRA, Marcela I. Protección de datos Personales: **Ley 25.326 y Dto. 1558/01 comentados - derecho constitucional provincial Iberoamérica y México**. Buenos Aires: Ediar, 2008(b).

BAUZÁ, Marcelo. **Manual de derecho informático e informática jurídica II.** Montevideo: Fundación de Cultura Universitaria, 2018.

BELLI, et. al. Hacia un modelo latino-americano de adecuación para la transferência internacional de datos personales. **Discussion paper presentado en la Computers, Privacy and Data Protection Conference Latin America (CPDP LatAm)**, 2023. Disponível em: https://cpdp.lat/wp-content/uploads/2023/07/doc-discusion-cpdplatam23-2.3.pdf. Acesso em: 2 nov. 2023.

BENNETT, Colin; RAAB, Charles D. **Revisiting "The Governance of Privacy":** Contemporary Policy Instruments in Global Perspective. 17 ago. 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972086. Acesso em: 2 nov. 2023.

BENNETT, Colin; RAAB, Charles D. **The governance of privacy: Policy instruments in global perspective**. First published 2003, Routledge Revivals, 2018(b).

BENKLER, Yochai. The wealth of networks: **how social production transforms markets and freedom**, New Haven and London: Yale University Press, 2006.

BERMAN, Paul Schiff. Cyberspace and the state action debate: the cultural value of applying constitutional norms to private regulation. **University of Colorado Law Review**, v. 71, 4 mai. 2000. pp. 1263-1310. Disponível: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=228466. Acesso em: 2 nov. 2023.

_____. The globalization of jurisdiction. **University of Pennsylvania Law Review**, v.151, n. 2, dez. 2002. pp. 311-545. Disponível: https://core.ac.uk/download/pdf/192849822.pdf. Acesso em: 2 nov. 2023.

_____. Global legal pluralism. **Southern California Law Review**, v. 80, n.6, 2007, pp. 1155-1238.

_____. Global legal pluralism as a normative project. **UC Irvine L. Rev**., v. 8, mar. 2018. pp. 149-181

BIONI, Bruno; MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 2a ed. São Paulo: Thomson Reuters, 2020.

BIONI, Bruno; ZANATTA, Rafael A.; RIELLI, Mariana. Caso: IBGE vs. CFOAB e outros (ADIs 6.387, 6.388, 6.389, 6.390 e 6.393). **Revista de Direito Civil Contemporâneo**, vol. 26, 2021, pp. 363-391.

BLACK, Julia. Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. Current Legal Problems, v. 54, n. 1, **Oxford University Press (OUP)**. fev. 2001, pp. 103-146. Disponível em: https://academic.oup.com/clp/article-abstract/54/1/103/400274?redirectedFrom=fulltext. Acesso em: 2 nov. 2023.

BLANCO GAITAN, David. Challenges of Colombian Data Protection Framework Towards a European Adequate Level of Protection. **University of Oslo**, 2019. Disponível em: https://www.duo.uio.no/handle/10852/68578. Acesso em: 2 nov. 2023.

BORCHE, Alejandro; SENA, Sonia. Incidencia de las leyes de protección de datos y acceso a la información pública en la gestión de la administración. **V Encontro Internacional do CONPEDI** Montevidéu, 2016. Disponível em: http://site.conpedi.org.br/publicacoes/4k6wgq8v/3dp0wv9s/T6i84x4b5KSHtPWx.pdf. Acesso em: 2 nov. 2023.

BRASIL. Constituição. **Constituição da República Federativa do Brasil**, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 2 nov. 2023.

_____. Lei nº 8.078/1990. **Dispõe sobre a proteção do consumidor e dá outras providências**. 11 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 2 nov. 2023.2023.

_____. Lei nº 9.507/1997, de 12 de novembro de 1997. **Regula o direito de acesso a informações e disciplina o rito processual do habeas data**. Diário Oficial da União - Seção 1 - 13/11/1997, Página 26025.. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9507.htm. Acesso em: 2 nov. 2023.

_____. Lei nº 12.414/2011. **Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito**. 9 jun. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 2 nov. 2023.

_____. Lei nº 12.527/2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências**. 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 2 nov. 2023.

_____. Lei nº 12.965/2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. 23 abr. 2014 Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 2 nov. 2023.

_____. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. **Diário Oficial da União**: seção 1, Brasília, DF, ano 139, n. 8, 14 ago 2018. pp. 1-74. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 2 nov. 2023.

_____. Lei Complementar nº 166/ 2019**. Altera a Lei Complementar nº 105, de 10 de janeiro de 2001, e a Lei nº 12.414, de 9 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores**. 8 abr. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp166.htm. Acesso em: 2 nov. 2023.

_____. Medida Provisória Nº 954/2020. **Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 2 nov. 2023.

_____. Emenda Constitucional nº 115/2022: **altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais**. 10 fev. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20Nº%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais. Acesso em: 2 nov. 2023.

_____. Ministério da Justiça e Segurança Pública. **Convenção de Budapeste é promulgada no Brasil,** 17 abr. 2023. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso em: 2 nov. 2023.

BUCKLAND, Michael. **Information and information systems**. Westport, CT: Praeger, 1991.

CANO, Lucero Galvis. El Panóptico digital de la protección de datos personales en Colombia. **Revista Temas**: Departamento de Humanidades Universidad Santo Tomás Bucaramanga, n. 12, 2018, pp. 125-140.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 2005.

CATE, Fred H.; DEMPSEY, James X.; RUBINSTEIN, Ira S. Systematic government access to private-sector data. **International Data Privacy Law**, v. 2, n. 4, 2012. pp. 195-199.

CAVOUKIAN, Ann. **Privacy by design: take the challenge**. Toronto: Information and privacy commissioner of Ontario (Canada), 1 jan. 2009.

CAVOUKIAN, Ann; TAYLOR, Scott; ABRAMS, Martin E. Privacy by design: essential for organizational accountability and strong business practices. **Identity in the Information Society**, v. 3, n. 2, ago. 2010. pp. 405-413. Disponível: https://core.ac.uk/download/pdf/81526429.pdf. Acesso em: 2 nov. 2023.

CIPL - CENTRE FOR INFORMATION POLICY LEADERSHIP. **What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework**. Report of the CIPL Accountability Mapping Project, mai. 2020. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_mapping_long_infographic.pdf. Acesso em: 2 nov. 2023.

_____. **APEC CBPR & PRP Questions and Answers**. 2020(b). Disponível em: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/03/cipl_cbpr_and_prp_q_a_final__19_march_2020_.pdf. Acesso em: 2 nov. 2023.

_____. **Data Localization and Government Access to Data Stored Abroad**. mar. 2023. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-tls_discussion_paper_ii_data_localization_and_government_access_to_data_stored_abroad__29_march_2023__2_.pdf. Acesso em: 2 nov. 2023.

CHANDER, Anupam; SCHWARTZ, Paul. Privacy and/or Trade. **U. Chi. L. Rev**., v. 90, 2023. p. 49.

CHANG, Lennon YC; GRABOSKY, Peter. The governance of cyberspace. In: DRAHOS, Peter (ed.), **Regulatory theory: foundations and applications**, Canberra: The Australian National University Press, 2017. pp. 533-551. Disponível em: https://library.oapen.org/bitstream/handle/20.500.12657/31596/1/626829.pdf. Acesso em: 2 nov. 2023.

COHEN, Julie E. What privacy is for. **Harv. L. Rev**., v. 126, 2012, pp. 1904-1933.

_____. Between truth and power: **the legal constructs of information capitalism**. New York: Oxford University Press, 2019.

COLOMBIA. Decreto nº 2591/1991**: por el cual se reglamenta la acción de tutela consagrada en el artículo 86 de la Constitución Política 1991**. Función Pública, 1991.

Disponível em: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=5304. Acesso em: 2 nov. 2023.

_____. Lei nº 222/1995. **Por la cual se modifica el Libro II del Código de Comercio, se expide un nuevo régimen de procesos concursales y se dictan otras disposiciones.** 20 dez. 1995. Disponível em: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6739. Acesso em: 2 nov. 2023.

_____. Ley Estatutaria 1.266/2008**. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones**. 31 dez. 2008. Disponível em: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488. Acesso em: 2 nov. 2023.

_____. Corte Constitucional. **Sentencia C-748/11. Proyecto de Ley Estatutaria de Habeas Data y Proteccion de Datos Personales. Control De Constitucionalidad de Los Proyecto de Ley Estatutaria,** 2011. Disponível em: http://www.secretariasenado.gov.co/senado/basedoc/c-748_2011.html#inicio. Acesso em: 2 nov. 2023.

_____. Ley Estatutaria nº 1.581/2012. **Por la cual se dictan disposiciones generales para la protección de datos personales: Función Pública,** ano 139, n. 8, 17 out 2012. p. 1-74,. Disponível em: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html. Acesso em: 2 nov. 2023.

_____. Decreto 1.377/2013**. Por el cual se reglamenta parcialmente la Ley 1581 de 2012**. 27 jun. 2013. Disponível em: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646. Acesso em: 2 nov. 2023.

_____. Ley 2157/2021. **Por medio de la cual se modifica y adiciona la Ley Estatutaria 1266 De 2008, y se dictan disposiciones generales del Habeas Data con relación a la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.** 29 out. 2021. Disponível em: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=173246. Acesso em: 2 nov. 2023.

_____. Decreto nº 255/2022**. Por el cual se adiciona la Sección 7 al Capítulo 25 del Título 2 de la Parte 2 del Libro 2 del Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, sobre normas corporativas vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países**. 23 fev. 2022. Diponível em: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=179087. Acesso em: 2 nov. 2023.

COMISSAO EUROPEIA. **Decisão da Comissão nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais na Argentina** (2003/490/CE). Bruxelas, 3 jun. 2003**.** Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003D0490. Acesso em: 2 nov. 2023.

_____. **Decisão da Comissão nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados** (2012/484/UE). Bruxelas, 12 ago. 2012**.** Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012D0484 Acesso em: 2 nov. 2023.

_____. **Commission implementing decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield C (2016) 4176 final**. Bruxelas, 12 jul. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG. Acesso em: 2 nov. 2023.

_____. Digital Single Market – **Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers**. 10 jan. 2017. Disponível em: https://ec.europa.eu/commission/presscorner/detail/de/MEMO_17_15. Acesso em: 2 nov. 2023.

_____. **Standard contractual clauses for data transfers between EU and non-EU countries**. 2021. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en. Acesso em: 2 nov. 2023.

_____. **Questions & Answers: EU-US Data Privacy Framework**. 10 jul. 2023. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752. Acesso em: 2 nov. 2023.

_____. **Commission implementing decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework**. Bruxelas, 10 jul. 2023. Disponível em: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf. Acesso em: 2 nov. 2023.

_____. **How the EU determines if a non-EU country has an adequate level of data protection**. 2023. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#adequacy-decisions-latest. Acesso em: 2 nov. 2023.

CONSELHO DA EUROPA. Treaty 108: **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. Estrasburgo, 28 jan. 1981. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108. Acesso em: 2 nov. 2023

_____. **Convention on Cybercrime**. Budapeste, Budapeste, 23 nov. 2001. Disponível em: https://www.coe.int/en/web/cybercrime/the-budapest-convention. Acesso em: 2 nov. 2023.

_____. **Additional protocol to Convention 108 regarding supervisory authorities and transborder data flows (ETS No. 181)**. Estrasburgo, 8 nov. 2001. Disponível em: https://rm.coe.int/1680080626. Acesso em: 2 nov. 2023.

_____. Treaty 189: **First Protocol on Xenophobia and Racism**. Estrasburgo, 2003. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189. Acesso em: 2 nov. 2023.

_____. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Request by Uruguay to be invited to accede**, 2011. Disponível em: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cce94. Acesso em: 2 nov. 2023.

_____. Treaty 223: **protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. Estrasburgo, 18 mai. 2018. Disponível:https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1. Acesso em: 2 nov. 2023.

_____. Treaty 224: **second additional protocol on enhanced co-operation**. Estrasburgo, 12 maio 2022. Disponível: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224. Acesso em: 2 nov. 2023.

_____. **Model Contractual Clauses for the Transfer of Personal Data from Controller to Controller**. 27 jun. 2023. Disponível em: https://www.coe.int/en/web/data-protection/-/model-contractual-clauses-for-the-transfer-of-personal-data. Acesso em: 2 nov. 2023.

_____. **Who are the Parties to the Budapest Convention?** 2023. Disponível em: https://www.coe.int/en/web/cybercrime/the-budapest-convention. Acesso em: 2 nov. 2023.

_____. Chart of signatures and ratifications of Treaty 108: **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. 2023. Disponível: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures. Acesso em: 2 nov. 2023.

_____. Chart of signatures and ratifications of Treaty 223: **protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. 2023 Disponível: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures. Acesso em: 2 nov. 2023.

_____. **Digital Partnerships**. 2023. Disponível em: https://rm.coe.int/leaflet-%20partnership-with-internet-companies-en/168079ced2%20. Acesso em: 2 nov. 2023

_____. Convention 108. **Treaty list for a specific State – Argentina**. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaties-full-list-signature&CodePays=ARG. Acesso em: 2 nov. 2023.

_____. **Convention 108. Treaty list for a specific State – Uruguay**. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaties-full-list-signature&CodePays=URU. Acesso em: 2 nov. 2023.

CORDEIRO, Nefi et alli. **Anteprojeto de Lei de proteção de dados para segurança pública e persecução penal. Brasília:** Poder 360, 2020. Disponível: https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf. Acesso em: 2 nov. 2023.

CORNELL LAW SCHOOL. Legal Information Project. **18 U.S. Code § 2523 - Executive agreements on access to data by foreign governments**. Ithaca, 2021. Disponível em: https://www.law.cornell.edu/uscode/text/18/2523. Acesso em: 2 nov. 2023.

CUMBRE IBEROAMERICANA. **XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno 14 y 15 de Noviembre**. Santa Cruz de la Sierra, 2003. Disponível em: https://www.segib.org/wp-content/uploads/DeclaraciondeSantaCruz.pdf. Acesso em: 2 nov. 2023.

DATA PROTECTION COMMISSION. **Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation**. Dublin: 22 maio 2023. Disponível em: https://edpb.europa.eu/our-work-tools/consistency-findings/register-decisions/2023/decision-data-protection-commission_en. Acesso em: 2 nov. 2023.

DAVENPORT, Thomas H.; PRUSAK, Laurence. Working knowledge: How organizations manage what they know. **Harvard Business Press**, 1998.

DELPIAZZO, Carlos E.; PASCALE, Maricarmen; PEÑA, Daniela; MELERAS, Flavia; SARAVIA. Andrés. **Protección de datos personales en Uruguay y el Mercosur**. Montevidéu: Fundación de Cultura Universitaria, 2005.

DONEDA, Danilo. Iguais mas separados: o Habeas data no ordenamento brasileiro e a proteção de dados pessoais. **Cadernos da escola de direito**, n. 9, 2008. p. 24-25 Disponível em: https://portaldeperiodicos.unibrasil.com.br/index.php/cadernosdireito/article/view/2607/2180. Acesso em: 2 nov. 2023.

_____. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**, v. 12, n. 2, 2011. pp. 91-108,.

_____. Da privacidade à proteção de dados. São Paulo: **Revista dos Tribunais**, 2019.

ESPANHA. **Ley Orgánica 5/1992 de regulación del tratamiento automatizado de los datos de carácter personal.** BOE núm. 262, de 31 de octubre de 1992. 29 out. 1992. pp. 37037 a 37045. Disponível em: https://www.boe.es/buscar/doc.php?id=BOE-A- 1992-24189. Acesso em: 2 nov. 2023.

_____. **Ley Orgánica 15/1999 de protección de datos de carácter personal**. BOE núm. 298, de 14/12/1999. 13 dez. 1999. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750. Acesso em: 2 nov. 2023.

ESTADOS UNIDOS. **Records, computers, and the rights of citizens**. Washington, DC: Department of Health, Education & Welfare, 1 jul. 1973. p. 193. pp. XX-XXI. Disponível: https://www.justice.gov/opcl/docs/rec-com-rights.pdf. Acesso em: 2 nov. 2023.

_____. **H.R.4943 – CLOUD Act – 115th Congress (2017-2018)**. Washington, 2 jun. 2018. Disponível: https://www.congress.gov/bill/115th-congress/house-bill/4943/text. Acesso em: 2 nov. 2023.

_____. **California Consumer Privacy Act of 2018**, Cal. Civ. Code §§ 1798.100 a 1798.199. Disponível em: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 Acesso em: 2 nov. 2023.

_____. The White House. **Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities (14086)**. Washington, 7 out. 2022. Disponível em: https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22531.pdf. Acesso em: 2 nov. 2023

_____. Department of Justice. **Attorney General designations of "qualifying states" under section 3(f) of EO 14086.** Washington, 2023. Disponível em: https://www.justice.gov/opcl/executive-order-14086. Acesso em: 2 nov. 2023.

_____. The White House. **Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence**. Washington, 30 jun. 2023. Disponível em: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/. Acesso em: 2 nov. 2023.

_____. The White House. **FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence**. Washington, 30 jun. 2023. Disponível em: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/. Acesso em: 2 nov. 2023.

EUROPEAN DATA PROTECTION BOARD. **Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679**. 25 mai. 2018. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf Acesso em: 2 nov. 2023.

_____. **Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.** 18 jun. 2021. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en. Acesso em: 2 nov. 2023.

FALIERO, Johanna C. La protección de los datos personales del consumidor y su importancia cardinal en nuestro sistema jurídico argentino. **Revista luso-brasileira de direito do consumo**, JM Editora, v. 7, n. 27, set. 2017. pp. 111-126.

FARRELL, Henry; NEWMAN, Abraham. The transatlantic data war: Europe fights back against the NSA. **Foreign Affairs**, v. 95, n. 1, jan/fev. 2016. pp. 124-133.

_____. Of privacy and power: **The transatlantic struggle over freedom and security**. Princeton University Press, 2 abr. 2019. pp. 248.

FEDERAL NETWORKING COUNCIL. Definition of "Internet". **Resolution of 24 October 1995**. Disponível em: https://www.nitrd.gov/historical/fnc/internet_res.pdf. Acesso em: 2 nov. 2023.

FEICK, Jürgen; WERLE, Raymund. Regulation of cyberspace. In: BALDWIN, Robert; CAVE, Martin; LODGE, Martin (Ed.). **The Oxford handbook of regulation**. Oxford Handbooks, 2010.

FERRAZ JUNIOR, Tercio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista Tributária e de Finanças Públicas**, São Paulo, v. 1, out. 1992.

FONSECA, Mariana Moutinho. The Federal Trade Commission Against Facebook: **a law and society approach to consumer privacy and competition policy**. Dissertação (Mestrado em Direito), Universidade de Brasília, Brasília, 2021. Disponível em:https://repositorio.unb.br/browse?type=author&value=Fonseca%2C+Mariana+Moutinho. Acesso em: 2 nov. 2023.

FRAZÃO, Ana. **Premissas para a reflexão sobre a regulação da tecnologia**. JOTA, 16 nov. 2017. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/premissas-para-a-reflexao-sobre-a-regulacao-da-tecnologia-16112017. Acesso em: 2 nov. 2023.

_____. Plataformas digitais, big data e riscos para os direitos da personalidade. In: TEPEDINO, Gustavo; MENEZES, Joyceane. **Autonomia privada, liberdade existencial e direitos fundamentais**. Belo Horizonte: Forum, 2019. pp. 333-349.

_____. Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 2ª ed. São Paulo: RT, 2020. pp.23-52.

FRAZÃO, Ana; SANTOS, Luiza Mendonça da Silva Belo. Plataformas Digitais e o Negócio de Dados: necessário diálogo entre o Direito da Concorrência e a Regulação dos Dados. **Direito Público**, v. 17, n. 93, 2020. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3695. Acesso em: 2 nov. 2023

FRENE, Lisandro. **El "encargado de tratamiento" de datos personales en el derecho argentino**. 14 mar. 2022. Disponível em: https://abogados.com.ar/el-encargado-de-tratamiento-de-datos-personales-en-el-derecho-argentino/30096. Acesso em: 2 nov. 2023.

GELLMAN, Robert. Can privacy be regulated effectively on a national level? Thoughts on the possible need for international privacy rules. **Villanova Law Review**, v. 41, 1996. pp. 129-172. Disponível: https://digitalcommons.law.villanova.edu/vlr/vol41/iss1/2/. Acesso em: 2 nov. 2023.

_____. **Fair Information Practices: a basic History**, 2022. p. 59. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020. Acesso em: 2 nov. 2023.

GIURGIU, Andra; LARSEN, Tine A. Roles and powers of national data protection authorities. **European Data Protection Law Review**, v. 2, n. 3, 2016. pp. 342-352. Disponível: https://www.semanticscholar.org/paper/Roles-and-Powers-of-National-Data-Protection-Giurgiu-_Larsen/fb3e33026e4a0e86eb55c64cf4888294ed5b9ed0?p2df. Acesso em: 2 nov. 2023.

GLOBAL CBPR FORUM. **Global Cross-Border Privacy Rules (CBPR) Declaration**. 21 abr. 2022. p. 2. Disponível em: https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-Declaration-2022.pdf. Acesso em: 2 nov. 2023.

_____.**Global Cross-Border Privacy Rules (CBPR) Framework (2023)**. 2023. Disponível em: https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-Framework-2023.pdf. Acesso em: 2 nov. 2023.

_____. **About the Global CBPR Forum**. 2023. https://www.globalcbpr.org/about/. Acesso em: 2 nov. 2023.

_____. **Global Forum Assembly, Annual Work Program, through April 2024.** 30 jun. 2023. Disponível em: https://www.globalcbpr.org/the-forum-releases-its-annual-work-program-for-2023-2024/. Acesso em: 2 nov. 2023.

GONZÁLEZ ALLONCA, Juan C.; RUIZ MARTÍNEZ, Esteban. Cloud Computing: la regulación de la transferencia internacional de datos personales y la prestación de servicios por parte de terceros. **Sistema Argentino de Información Jurídica – Ministerio de Justicia y Derechos Humanos**. 1 out. 2015. Disponível em: http://www.saij.gob.ar/. Acesso em: 2 nov. 2023.

GREAT BRITAIN, Home Office, **Report of the Committee on Privacy**. Rt. Hon. Kenneth Younger, Chairman (London: H. M. Stationery Office), 1972.

GREENLEAF, Graham. Global data privacy laws 2023: 162 national laws and 20 Bills. **181 Privacy Laws and Business International Report (PLBIR),** 1, 2-4, 6 fev. 2023. Disponível em: https://www.privacylaws.com/reports-gateway/articles/int181/int181_2023/. Acesso em: 2 nov. 2023.

_____. **Asian data privacy laws: trade & human rights perspectives**. OUP Oxford, 16 dez. 2014. p. 624.

GSTREIN, Oskar Josef. The Council of Europe as an Actor in the Digital Age: Past Achievements, Future Perspectives. **Festschrift der Mitarbeiter Innen und Doktorand Innen zum**, v. 60, 2019. pp. 75-90.

GUADAGNA, Bruno Gaiero; BRACESCO, Ignacio M. Soba. El proceso de hábeas data en el Uruguay (protección de datos personales y acceso a la información pública). **Anuario de Derecho Constitucional Latinoamericano**. Montevideo, 2010. pp. 326-349. Disponível em: https://www.corteidh.or.cr/tablas/r28363.pdf. Acesso em: 2 nov. 2023.

GUZMAN, Andrew T.; MEYER, Timothy L. International soft law. **Journal of Legal Analysis**, v. 2, n. 1, 2010. pp. 171-225.

HEISENBERG, Dorothee. Negotiating Privacy: The European Union, the United States, and Personal Protection. **Lynne Rienner Publishers**, 2005.

HELBERGER, Natali; BORGESIUS, Frederik Zuiderveen; REYNA, Agustin. The perfect match? A closer look at the relationship between EU consumer law and data protection law. **Common Market Law Review**, v. 54, n. 5, 2017. pp. 28.

HOOD, Christopher. The tools of government in the information age. In: MORAN, Michael; REIN, Martin; GOODIN, Robert E. (Ed.). **The Oxford handbook of public policy**. Oxford University Press, 2008. pp. 469–481.

IT GOVERNANCE. **ISO 27700 Privacy Information management system**. Green paper. 2023. Disponível em: https://www.itgovernance.co.uk/iso-27701. Acesso em: 2 nov. 2023.

JOERGES, Christian; SAND, Inger-Johanne; TEUBNER, Gunther (Ed.). **Transnational governance and constitutionalism**. Hart Publishing, 2004.

JOHNSON, David R.; POST, David. Law and borders: The rise of law in cyberspace. **Stanford law review**, 1996. pp. 1367-1402,

KELLER, Clara Iglesias. Entre exceção e harmonização: o debate teórico sobre a regulação da Internet| Between exception and harmonization: the theoretical debate on Internet regulation. **Revista Publicum**, v. 5, n. 1, 2019. pp. 137-166

KUNER, Christopher. Regulation of transborder data flows under data protection and privacy law: past, present, and future. **TILT Law & Technology,** Working Paper, n. 016, 10 out. 2010. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1689483. Acesso em: 2 nov. 2023.

_____. The Internet and the global reach of EU law. In: CREMONA, Marise and SCOTT, Joanne (Eds.), **EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law**, 2017. pp. 112-145.

_____. Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection. **University of Cambridge Faculty of Law**, Research Paper, n. 20, 2021.

LESSIG, Lawrence. **Code: version 2.0**. Nova Iorque: Basic Books, 2006.

LLOYD, Ian J. **Information Technology Law**. Oxford: Oxford University Press, 2017.

LYNSKEY, Orla. **The foundations of EU data protection law**. Oxford University Press, 2015.

MAFFINI, Rafael; CARVALHO, Luciana Luso de. A atribuição do regime autárquico especial à Autoridade Nacional de Proteção de Dados. **Revista de Direito do Consumidor**, v. 144, 2022.

MARSDEN, Christopher T. **Internet Co-regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace.** Cambridge: Cambridge University Press, 18 ago. 2011.

MARTINÉZ, Esteban Ruiz. Protección de los datos personales en los informes creditícios: **delitos contra la intimidad informática**. Buenos Aires: Hammurabi. 2015. p. 61.

MAYER-SCÖNBERGER. General development of data protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). **Technology and privacy: The new landscape**. Cambridge: MIT Press, 1997. pp. 219-241.

MAYER-SCHÖNBERGER, Viktor. CUKIER, Kenneth. Big Data: **como extrair volume, variedade, velocidade e valor da avalanche de informações cotidianas**. Rio de Janeiro, Elsevier. 2013. Tradução Paulo Polzonoff Junior.

MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados de uma mesma moeda. **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 12, n. 39, 2018. pp. 185-216.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, v. 120, 2018. p. 555.

_____. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, 2020. p. 15.

MENDES, Laura Schertel; DA FONSECA, Gabriel C. Soares. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **REI-Revista Estudos Institucionais**, v. 6, n. 2, mai/ago. 2020. pp. 507-533.

_____. STF reconhece direito fundamental à proteção de dados. **Revista de Direito do Consumidor**, vol. 130, 2020.

MERCOSUL. **Tratado de Assunção para a Constituição de um Mercado Comum**. Assunção, 1991. p. 30. Disponível em: https://www.mercosur.int/documento/tratado-de-assuncao-para-a-constituicao-de-um-mercado-comum/. Acesso em: 2 nov. 2023.

_____. **XII Reunion ordinaria del subgrupo de trabajo n. 13 – Comercio Electronico**, 2004. Disponível em: https://documentos.mercosur.int/simfiles/docreuniones/23116_SGT13_2004_ACTA02_ES.pdf. Acesso em: 2 nov. 2023.

_____. **Decisão sobre a suspensão da Venezuela no MERCOSUL**. 5 ago. 2017. Disponível em: https://www.mercosur.int/pt-br/decisao-sobre-a-suspensao-da-republica-bolivariana-da-venezuela-no-mercosul/. Acesso em: 2 nov. 2023.

_____. **Decisão no 15/20: Acordo sobre Comércio Eletrônico do Mercosul**. Conselho do Mercado Comum (CMC), 29 abr. 2021. Disponível em: https://www.mercosur.int/documento/acordo-sobre-o-comercio-eletronico-do-mercosul/. Acesso em: 2 nov. 2023.

_____. **Agenda Digital**. 2023. Disponível em: https://www.mercosur.int/pt-br/temas/agenda-digital/. Acesso em: 2 nov. 2023.

_____ **Países do MERCOSUL**. 2023. Disponível em: https://www.mercosur.int/pt-br/quem-somos/paises-do-mercosul/. Acesso em: 2 nov. 2023.

_____. **Objetivos do MERCOSUL**. 2023. Disponível em: https://www.mercosur.int/pt-br/quem-somos/objetivos-do-mercosul/. Acesso em: 2 nov. 2023.

MILLARD, Christopher J. **Cloud computing law**. Oxford: Oxford University Press, 2021.

MURRAY, Andrew. Nodes and gravity in virtual space. **Legisprudence: International Journal for the Study of Legislation, Hart Pub**, v. 5, n. 2. 2001. pp. 195-221.

_____. The regulation of cyberspace**: control in the online environment**. Routledge, 2007.

_____. Conceptualising the Post-Regulatory (Cyber)state In: BROWNSWORD, Roger, YEUNG, Karen (org). **Regulating technologies: legal futures, regulatory frames and technological fixes**. Oxford, Hart, 2008

NAEF, Tobias. **Data Protection Without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law**. Springer Nature, 13 dez. 2023.

NISSENBAUM, Helen. **Privacy in context: Technology, policy, and the integrity of social life**. Stanford University Press, 2020.

OCDE - ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Convention on the Organisation for Economic Cooperation and Development.** Paris, 14 dez. 1960. Disponível em: https://www.oecd.org/about/document/oecd-convention.htm. Acesso em: 2 nov. 2023

_____. **OECD Privacy Guidelines**. Paris, 23 set. 1980. Disponível: https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en. Acesso em: 2 nov. 2023

_____. **Thirty years after the OECD privacy guidelines**. Paris, 6 abr. 2011(a). p. 49. Disponível em: http://dx.doi.org/10.1787/5kgf09z90c31-en. Acesso em: 2 nov. 2023.

_____. Report on the Implementation of the OECD. **Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy**. Paris, 27 abr. 2011(b). p. 23. Disponível em: http://dx.doi.org/10.1787/5kgdpm9wg9xs-en. Acesso em: 2 nov. 2023.

_____. **The OECD privacy framework**. Paris, 2013. p. 154. Disponível: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso em: 2 nov. 2023

_____. **Colombia's path towards OECD accession**. 15 jan. 2020. Disponível em: https://www.oecd.org/colombia/colombia-accession-to-the-oecd.htm. Acesso em: 2 nov. 2023

_____. **OECD takes first step in accession discussions with Argentina, Brazil, Bulgaria, Croatia, Peru and Romania**. 25 jan. 2022. Disponível em: https://www.oecd.org/newsroom/oecd-takes-first-step-in-accession-discussions-with-argentina-brazil-bulgaria-croatia-peru-and-romania.htm. Acesso em: 2 nov. 2023.

_____. Moving forward on data free flow with trust**: new evidence and analysis of business experiences**. OECD Digital Economy Papers, n. 353. Paris, OCDE, 2023. Disponível em: https://www.oecd-ilibrary.org/science-and-technology/moving-forward-on-data-free-flow-with-trust_1afab147-en. Acesso em: 2 nov. 2023.

PALAZZI, Pablo A. La transmisión internacional de datos personales y la protección de la privacidade: **Argentina, América Latina, Estados Unidos y Unión Europea**. Buenos Aires: Ad-hoc, 2002.

PASQUALE, Frank. **The black box society**. The secret algorithms that control money and information. Cambridge: Harvard University Press. 2015.

PUCCINELLI, Oscar Raúl. Evolución histórica y análisis de las diversas especies, subespecies, tipos y subtipos de habeas data en América Latina. Un intento clasificador con fines didácticos. **Vniversitas**, n. 107, 2004. pp. 471-501.

REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. **Padrões de Proteção de Dados Pessoais para os Estados Ibero-americanos**. 20 jun. 2017. Disponível em: https://www.redipd.org/sites/default/files/inline-files/Estandares_PORTUGUES.pdf. Acesso em: 2 nov. 2023.

_____. **Regulamento da Rede Ibero-americana de Proteção de Dados (RIPD)**. 2018. Disponível em: https://www.redipd.org/sites/default/files/inline-files/REGLAMENTO_RIPD_REV30_11_18_PT.pdf. Acesso em: 2 nov. 2023

_____. **Guia para a Implementação de Cláusulas Contratuais Modelo para a Transferência Internacional de Dados Pessoais (TIDP).** 2021. Disponível em: https://www.redipd.org/sites/default/files/2023-02/guia-implementacion-clausulas-contractuales-modelo-tidp-pt.pdf. Acesso em: 2 nov. 2023.

_____. **Modelos de Cláusulas Contratuais**. 2021. Disponível em: https://www.redipd.org/sites/default/files/2023-02/anexo-modelos-clausulas-contractuales-pt.pdf. Acesso em: 2 nov. 2023. p.47.

_____. **Historia de la Red Iberoamericana de Protección de Datos (RIPD)**. 2023. Disponível em: https://www.redipd.org/es/la-red/historia-de-la-red-iberoamericana-de-proteccion-de-datos-ripd. Acesso em: 2 nov. 2023.

_____. **Órganos de la Red Iberoamericana de Protección de Datos**. 2023. Disponível em: https://www.redipd.org/es/la-red/organos-de-la-red-iberoamericana-de-proteccion-de-datos. Acesso em: 2 nov. 2023.

_____. **Relación de entidades integrantes de la RIPD**. 2023. Disponível em: https://www.redipd.org/es/la-red/entidades-acreditadas. Acesso em: 2 nov. 2023.

REIDENBERG, Joel R. Governing networks and rulemaking in Cyberspace. **Emory Law Journal**, v. 45, 1996. p. 911-930. Disponível: https://ir.lawnet.fordham.edu/faculty_scholarship/29. Acesso em: 2 nov. 2023.

_____. Lex informatica: The formulation of information policy rules through technology. **Texas Law Review**, v. 76, n. 3, 1998. pp. 553-593. Disponível: https://core.ac.uk/download/pdf/144222024.pdf. Acesso em: 2 nov. 2023.

REIGADA, Antonio Troncoso. El desarrollo de la protección de datos personales em Iberoamérica desde una perspectiva comparada y el reequilibro en los modelos de datos a nível internacional. **Revista Internacional de Protección de Datos Personales**, n. 1. dez. 2012. pp. 4-41. Disponível em: https://habeasdatacolombia.uniandes.edu.co/wp content/uploads/10_Antonio-troncoso_FINAL.pdf. Acesso em: 2 nov. 2023.

REMOLINA, Nelson. ¿ Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?. **International Law**, n. 16, 2010. pp. 489-523.

_____. Recolección internacional de datos personales: **un reto del mundo post-internet**. XVIII Edición del Premio Protección de Datos Personales de Investigación. Madrid: Agencia Española de Protección de Datos, 2015.

RIGAUDIAS, Cecilia Álvarez. Personal Data Protection. In.: MARTINEZ, Aurelio López-Tarruella; MIRETE, Carmen María García (Org.). **Derecho TIC: derecho de las tecnologías de la información y de la comunicación**, 2016. pp. 363-403.

RODOTÀ, Stefano. **El derecho a tener derechos**. Madrid: Trotta, 2014. ROJAS BEJARANO, Marcela. Evolución del derecho de protección de datos personales en colombia respecto a estándares internacionales. **Novum Jus**, 8 (1), 2014, pp. 107-139. Disponível em: https://repository.ucatolica.edu.co/entities/publication/b8054942-c619-46cc-8e58-46039f6ec2b6. Acesso em: 2 nov. 2023.

SAJFERT, Juraj; QUINTEL, Teresa. **Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities**. 2017. pp.22. Disponível em: https://ssrn.com/abstract=3285873 ou http://dx.doi.org/10.2139/ssrn.3285873. Acesso em: 2 nov. 2023.

SALINAS, Maria de Lourdes Zamudio. El marco normativo latinoamericano y la ley de protección de datos personales del Perú. **Revista Internacional de Protección de Datos Personales**, n. 1, jul./dez. 2012. p. 1-21. Disponível em: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok3_Ma.-de-Lourdes-Zamudio_FINAL.pdf. Acesso em: 2 nov. 2023.

SALT, Marcos. Nuevos desafios de la evidencia digital: **acceso transfronterizo y técnicas de acesso remoto a datos informáticos**. Buenos Aires: AdHoc, 2017.

SARASOLA, Florencia. **Ley de Protección de Datos Personales**. Universidad ORT Uruguay, Facultad de Ingeniería. Montevidéu, 2009. Disponível em: https://silo.tips/download/ley-de-proteccion-de-datos-personales-3. Acesso em: 2 nov. 2023.

SCHWARTZ, Paul M. Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices. **Wisconsin Law Review**, 2000. pp. 743-788.

_____. **Managing Global Data Privacy: Cross-Border information flows in a networked environment**. Privacy Projects, 2009. Disponível em: https://paulschwartz.net/wp-content/uploads/2019/01/Global_Data_Flows.pdf. Acesso em: 2 nov. 2023.

_____. Information privacy in the cloud. **U. Pa. L. Rev**., v. 161, p. p. 2012. p. 1623.

_____. The EU-US privacy collision: a turn to institutions and procedures. **Harvard Law Review.** v. 126, 2012. p. 1966.

_____. Global data privacy: The EU way. **NYUL Rev**., v. 94, 2019. p. 771.

SCHWARTZ, Paul M.; PEIFER, Karl-Nikolaus. Transatlantic data privacy law. **Georgetown Law Journal**, v. 106, n. 1, 2017. p. 115-179.

SIC - SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**. Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability)**. 2016. Disponível em: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf. Acesso em: 2 nov. 2023.

_____. **Guía para Solicitar la Declaración de Conformidad sobre las Transferencias Internacionales de Datos Personales.** 2016. Disponível em: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Guia_para_solicitar_la_declaracion_de_conformidad_sobre_las_trasferencias_internacionales_de_datos_personales.pdf. Acesso em: 2 nov. 2023.

_____. **Guía para la Implementación del Principio de Responsabilidad Demostrada en las Transferencias Internacionales de Datos Personales**. 2021. Disponível em: https://www.sic.gov.co/sites/default/files/files/2021/2021%20Gu%C3%ADas%20para%20implementación%20del%20principio%20de%20responsabilidad%20demostrada%202021.pdf. Acesso em: 2 nov. 2023.

_____. **Título V Protección de Datos Circular Única**. 2022 Disponível em: https://www.sic.gov.co/sites/default/files/normatividad/092022/T%C3%ADtulo%20V%20Versión%2029-09-2022.pdf. Acesso em: 2 nov. 2023.

SIMÃO, Bárbara; et al. Autoridades de Proteção de Dados na América Latina**: um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai**. São Paulo, IDEC, 2019. p. 12. Disponível em: https://idec.org.br/publicacao/autoridade-de-protecao-de-dados-na-america-latina. Acesso em: 2 nov. 2023.

SOLOVE, Daniel J.; SCHWARTZ, Paul M. **Information privacy law**. Aspen Publishing, 2020.

SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019.

SRNICEK, Nick. **Platform capitalism**. Cambridge, UK; Malden, MA: Polity Press, 2017.

STIGLITZ, Joseph. **People, power, and profits: Progressive capitalism for an age of discontent**. Penguin UK, 2019.

STUCKE, Maurice E. Should we be concerned about data-opolies?. **Georgetown Law Technology Review**, v. 2, 2017. p. 275.

TRAVIESO, Juan Antonio. **Régimen juridico de los datos personales. Hábeas data, cloud computing, responsabilidad, delitos, internet, redes, biometria**. Buenos Aires: Abeledo Perrot, 2014.

TREACY, Bridget; BAPAT, Anita. The Internet of Things – already in a home near you? **Privacy and Data Protection,** v. 14, n. 2, 2013. pp. 11-13. Disponível em: https://www.hunton.com/images/content/3/4/v2/3421/The_Internet_of_Things_already_in_a_home_near_you.pdf. Acesso em: 2 nov. 2023.

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**. Bruxelas, 24 out. 1995. Disponível: http://data.europa.eu/eli/dir/1995/46/oj. Acesso em: 2 nov. 2023.

_____. Working Party. **Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government (5092/98/EN/final/WP15)**, 26 jan. 1999. Disponível: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp15_en.pdf. Acesso em: 2 nov. 2023.

_____. **Carta dos Direitos Fundamentais da União Europeia.** (2000/C 364/01). Bruxelas, 18 dez. 2000. Disponível: http://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 2 nov. 2023.

_____. Comissão das Comunidades Europeias. **2000/520/CE: decisão da Comissão, de 26 de Julho de 2000, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de proteção assegurado pelos princípios de "porto seguro" e pelas respectivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América.** Bruxelas, 26 jul. 2000. Disponível: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32000D0520. Acesso em: 2 nov. 2023.

_____. Article 29 Data Protection Working Party. **Opinion 4/2002 on the level of protection of personal data in Argentina (11081/02/EN/Final WP 63)**. Bruxelas, 3 out. 2002. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm. Acesso em: 2 nov. 2023.

_____. Article 29 Data Protection Working Party. **Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay (0475/10/EN WP 177).** Bruxelas, 12 out. 2010. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp177_en.pdf. Acesso em: 2 nov. 2023.

_____. Tribunal de Justiça. **Acórdão (Grande Seção) de 6 out. 2015: Maximillian Schrems contra Data Protection Commissioner (processo C-362/14)**. Luxemburgo, 6 out. 2015. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62014CJ0362. Acesso em: 2 nov. 2023.

_____. **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)**. Bruxelas, 27 abr. 2016. Disponível: http://data.europa.eu/eli/reg/2016/679/oj. Acesso em: 2 nov. 2023.

_____. **Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho**. Bruxelas, 27 abr. 2016. Disponível: http://data.europa.eu/eli/dir/2016/680/oj. Acesso em: 2 nov. 2023.

_____. **Tratado sobre o Funcionamento da União Europeia.** (2016/C 202/01). EUR-Lex, 7 jun. 2016. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF. Acesso em: 2 nov. 2023.

_____. Tribunal de Justiça. Acórdão do Tribunal de Justiça (Grande Secção) de 16 de julho de 2020 - **Data Protection Commissioner contra Facebook Ireland Ltd e Maximillian Schrems - Processo C-311/18**. Luxemburgo, 16 jul. 2020. Disponível: http://curia.europa.eu/juris/liste.jsf?num=C-311/18. Acesso em: 2 nov. 2023.

URBINA, Francisco Zúñiga. Derecho a la intimidad y Hábeas Data (del recurso de protección al Hábeas Data). **Derecho PUCP**, v. 51, 1997.

URCDP. UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES. Resolución nº 4/2019: **Se resuelve sobre los países adecuados para transferencias internacionales de datos, sustituyendo la Resolución N° 17/009, de 12 de junio de 2009**. 12 mar. 2019. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-4019 . Acesso em: 2 nov. 2023.

_____. Resolución nº 41/2021**. se resuelve sobre lo dispuesto por el artículo 23 de la Ley N° 18.331, de 11 de agosto de 2008 respecto a las transferencias internacionales a territorios no adecuados.** 8 set. 2021. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-41021. Acesso em: 2 nov. 2023.

_____. **Nueva ley que aprueba el Convenio 108+**. 9 abr. 2021. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/noticias/nueva-ley-aprueba-convenio-108. Acesso em: 2 nov. 2023.

_____. Resolución nº 23/2021: **se resuelve sobre la necesidad de actualizar la Resolución Nº 4/019, de 12 de marzo de 2019, sobre los países u organizaciones**

consideradas adecuadas para las transferencias internacionales de datos, de conformidad con lo establecido por el artículo 23 de la Ley Nº 18.331, de 11 de agosto de 2008. 8 jun. 2021. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-23021. Acesso em: 2 nov. 2023.

_____. **Guía General de Protección de Datos Personales en Uruguay**. 24 jan. 2022. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-general-proteccion-datos-personales-uruguay. Acesso em: 2 nov. 2023.

_____. Resolución n° 50/2022**. Se resuelve sobre la publicación de la "Guía de Implementación de Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales (TIPD)" por la Red Iberoamericana de Protección de Datos (RIPD)**. 29 nov. 2022. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-50022. Acesso em: 2 nov. 2023.

_____. **Solicitud de transferencias Internacionales**. 29 set. 2023. https://www.gub.uy/tramites/solicitud-transferencias-internacionales. Acesso em: 2 nov. 2023.

URUGUAI. **Constitución de la Republica**, de 1967. Disponível em: https://parlamento.gub.uy/documentosyleyes/constitucion. Acesso em: 2 nov. 2023.

_____. **Ley 17.838/2004 de Protección de Datos Personales para ser utilizados en Informes Comerciales y Acción de Hábeas Data**. 24 set. 2004. Disponível em: https://www.impo.com.uy/bases/leyes-originales/17838-2004. Acesso em: 2 nov. 2023.

_____. **Ley nº 18.331 de 2008. Ley de Protección de Datos Personales. Registro Nacional de Leyes y Decretos**, Motevidéo, ano 2008, tomo 1, semestre 2, p. p. 18 ago. 2008. p. 378. Disponível em: https://www.impo.com.uy/bases/leyes/18331-2008. Acesso em: 2 nov. 2023.

_____. **Decreto 414/2009: reglamentacion de la Ley 18.331. Relativo a la Proteccion de Datos Personales**. 5 out. 2009. Disponível em: https://www.impo.com.uy/bases/decretos/414-2009. Acesso em: 2 nov. 2023.

_____. **Ley 18.381/2008: sobre el Derecho de Acceso a la Informacion Publica**. Registro Nacional de Leyes y Decretos. 7 nov. 2008. Disponível em: https://www.impo.com.uy/bases/leyes/18381-2008/9. Acesso em: 2 nov. 2023.

_____. **Ley 19.670/2018, de 25 de outubro de 2018. Aprobación de rendición de cuentas y balance de ejecución presupuestal.** 2018. Disponível em: https://www.impo.com.uy/bases/leyes/19670-2018. Acesso em: 2 nov. 2023.

_____. **Decreto 64/2020: reglamentación de los arts. 37 a 40 de la Ley 19.670 y art. 12 de la Ley 18.331/2008 a proteccion de datos personales**. Registro Nacional de Leyes y Decretos. 21 fev. 2020. Disponível em: https://www.impo.com.uy/bases/decretos/64-2020. Acesso em: 2 nov. 2023.

_____. Ministerio de Relaciones Exteriore. **Uruguay es invitado por el Consejo de Europa a adherir al Convenio de Budapest sobre Ciberdelincuencia**. 14 fev. 2023

Disponível em: https://www.gub.uy/ministerio-relaciones-exteriores/comunicacion/comunicados/uruguay-es-invitado-consejo-europa-adherir-convenio-budapest-sobre. Acesso em: 2 nov. 2023.

VÁSQUEZ VÉLEZ, Alejandra. **El ámbito de aplicación del régimen jurídico colombiano para la protección de datos personales. Su alcance frente a empresas extranjeras sin representación jurídica en Colombia**. Monografía jurídica para optar por el título de Abogada. Facultad de Ciencias Jurídicas Pontificia Universidad Javeriana, 2021. Disponível em: https://repository.javeriana.edu.co/handle/10554/58083. Acesso em: 2 nov. 2023.

VERONESE, Alexandre. The right of explanation and the right to object automatic decisions: **comparing the European Union General Data Protection Regulation (EU/GDPR) with the Brazilian General Data Protection Federal Act (BGDPFA)**. CPR LATAM Conference, Cordoba, Argentina, 2019. Disponível em: https://www.researchgate.net/publication/333599973_The_right_of_explanation_and_the_right_to_object_automatic_decisions_comparing_the_European_Union_General_Data_Protection_Regulation_EUGDPR_with_the_Brazilian_General_Data_Protection_Federal_Act_BGDPF. Acesso em: 2 nov. 2023.

_____. Transferências internacionais de dados pessoais: o debate transatlântico norte e sua repercussão na América Latina e no Brasil. In: MENDES, Laura Schertel (coord.); DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); RODRIGUES JR., Otavio Luiza (coord.); BIONI, Bruno (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro Editora Forense, 2021. pp. 689-726.

VERONESE, Alexandre; MELO, Noemy. A proposta brasileira de proteção de dados pessoais e comparação ao novo regulamento europeu. **Revista de Direito Civil Contemporâneo**, vol. 14, 2018.

VERONESE, Alexandre; SANTOS, Luiza Mendonça da Silva Belo. Padrões de conformidade nacionais de proteção de dados pessoais: anotações na perspectiva de compliance após a invalidação do privacy shield firmado entre os Estados Unidos da América e a Uninão Europeia. In: CUÊVA, Ricardo; FRAZÃO, Ana, **Compliance e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021.

VERONESE, Alexandre; CALABRICH, Bruno. Crimes na internet e o Brasil no cenário de cooperação jurídica internacional: **a convenção de Budapeste e o Cloud Act dos Estados Unidos**. JOTA, 24 abr. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/judiciario-e-sociedade/crimes-na-internet-e-o-brasil-no-cenario-de-cooperacao-juridica-internacional-24042021. Acesso em: 2 nov. 2023.

VERONESE, Alexandre, et al. Pesquisa documental e de campo sobre autoridades de proteção de dados na América Latina: **o conceito social e institucional de privacidade e de dados pessoais**. 2022, Biblioteca Virtual da FAPESP. Disponível em: https://bv.fapesp. br/en/auxilios/105576/documentary-and-field-research-on-the-latin-american-data-protection-authorities-the-social-and-inst/. Acesso em: 2 nov. 2023.

VIOLA, Mario et al. **O anteprojeto da LGPD Penal e as regras sobre transferência internacional de dados pessoais**. Instituto de Tecnologia & Sociedade do Rio em parceria com a Embaixada Britânica no Brasil. Ago. 2021. p. 28. Disponível em:

https://itsrio.org/pt/publicacoes/o-anteprojeto-da-lgpd-penal-e-as-regras-sobre-transferencia-internacional-de-dados-pessoais/. Acesso em: 2 nov. 2023.

VIOLA, Mario; FRANCA, Marcílio; DONEDA, Danilo. **Festa para a proteção de dados na América do Sul**. ConJur, 17 fev. 2021. Disponível em: https://www.conjur.com.br/2021-fev-17/opiniao-festa-protecao-dados-america-sul. Acesso em: 2 nov. 2023

WACKS, Raymond. **Personal information**. Oxford: Clarendon Press, 1989.

WEBER, Rolf H. Legal Interoperability as a Tool for Combatting Fragmentation. **Global Commission on Internet Governance**, Paper Series n. 4, dez. 2014. Disponível em: https://www.cigi*online*.org/sites/default/files/gcig_paper_no4.pdf. Acesso em: 2 nov. 2023.

WEISS, Martin A.; ARCHICK, Kristin. **US-EU data privacy: from safe harbor to privacy shield**. Washington, DC: Congressional Research System, 19 mai. 2016. p. 7. Disponível em: https://www2.epic.org/crs/R44257.pdf. Acesso em: 2 nov. 2023.

WORLD ECONOMIC FORUM. **Personal Data: The Emergence of a New Asset Class**. 2011. Disponível em: https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf Acesso em: 2 nov. 2023.

WU, Tim. Is Internet Exceptionalism Dead? In: SZOKA, Berim e MARCUS, Adam (Eds.) The Next Digital Decade: **essays on The Future of Internet**. Washington DC: TechFreedom 2010. pp. 179-188.

ZITTRAIN, Jonathan. **The future of the internet and how to stop it**. Yale University Press, 2008.

ZUBOFF, Shoshana. The age of surveillance capitalism**: the fight for a human future at the new frontier of power**. New York: PublicAffairs, 2019.