Luca Belli
Ana Brian Nougrères
Jonathan Mendoza Iserte
Pablo Andrés Palazzi
Nelson Remolina Angarita

Transferência Internacional de Dados Pessoais na América Latina

RUMO À HARMONIZAÇÃO DE NORMAS

Lumen Juris Direito | 35 anos

Transferência Internacional de Dados Pessoais na América Latina

Lumen Juris Editora

www.lumenjuris.com.br

Filiais

Sede: Rio de Janeiro
Rua Newton Prado, nº 43
CEP: 20930-445
São Cristóvão
Rio de Janeiro – RJ
Tel. (21) 2580-7178

Maceió
(Divulgação)
Cristiano Alfama Mabilia
cristiano@lumenjuris.com.br
Maceió – AL
Tel. (82) 9-9661-0421

Luca Belli
Ana Brian Nougrères
Jonathan Mendoza Iserte
Pablo Andrés Palazzi
Nelson Remolina Angarita

Transferência Internacional de Dados Pessoais na América Latina

RUMO À HARMONIZAÇÃO DE NORMAS

FGV DIREITO RIO

Editora Lumen Juris
Rio de Janeiro, 2024

Categoria: Direito Digital

Editor: João Luiz da Silva Almeida
Produção editorial: Angel Cabeza
Designer editorial: Rebecca Ramos e Thassiel Melo
Diagramação: Rômulo Lentini
Gerente administrativo-financeiro: Carla Sampaio
Financeiro: Juliano de Oliveira
Assistente financeiro: Jefferson Badaró
Gerente comercial e logística: Arlei Rocha
Comercial e relacionamento: Cristiano Mabilia
Eventos: Arianna Pacheco

Impresso no Brasil | *Printed in Brazil*

Dados Internacionais de Catalogação na Publicação (CIP)

T772

Transferência internacional de dados pessoais na América Latina : rumo à harmonização de normas / Luca Belli... [et. al]. – 1. ed. – Rio de Janeiro : Lumen Juris, 2024.
294 p. ; 23 cm.

ISBN 978-85-519-3246-9

1. Proteção de dados - Legislação. 2. Direito à privacidade. 3. Regulação. 4. Direito internacional – América Latina. I. Belli, Luca (autor). II. Título.

CDD 342.0858

Ficha catalográfica elaborada por Ellen Tuzi CRB-7: 6927

Editora Lumen Juris
Rua Newton Prado, 43, São Cristóvão, Rio de Janeiro/RJ
CEP: 20930-445
Telefone: (21) 2580-7178 | atendimento@lumenjuris.com.br

Biografia dos autores

Luca Belli

Professor de Governança e Regulação Digital na Escola de Direito da Fundação Getulio Vargas (FGV), no Rio de Janeiro, onde dirige o Centro de Tecnologia e Sociedade (CTS-FGV) e o projeto CyberBRICS. Luca também é editor da revista *International Data Privacy Law* (IDPL), publicada pela Oxford University Press, e diretor da conferência *Computers Privacy and Data Protection Latin-America* (CPDP LatAm). Atualmente, é membro do Comitê Nacional de Cibersegurança da Presidência do Brasil, membro do comitê diretivo da *Global Digital Inclusion Partnership* e membro do comitê diretivo do Fórum para a Informação e a Democracia. É autor de mais de 80 publicações sobre direito e tecnologia, que exploram o acesso à Internet, governança de dados, cibersegurança, regulação da IA e transformação digital. Foi consultado por várias organizações intergovernamentais e reguladores nacionais, e seus trabalhos foram citados por diversos meios de comunicação, incluindo *The Economist, Financial Times, Forbes, Le Monde, BBC, China Today, The Beijing Review, The Hill,* O *Globo*, *Folha de S.Paulo, El País e La Stampa*. Luca possui doutorado em Direito Público pela Universidade Paris Panthéon-Assas e pode ser encontrado no LinkedIn e Twitter como @1lucabelli.

Ana Brian Nougrères

Foi designada Relatora Especial das Nações Unidas em matéria de Privacidade pelo Conselho de Direitos Humanos das Nações Unidas em 1º de agosto de 2021. Doutora em Direito e Ciências Sociais pela Faculdade de Direito da Universidade da República Oriental do Uruguai e exerce a profissão de forma liberal desde então. Ensina os fundamentos do direito informático e da proteção de dados pessoais para estudantes da Facultad de Derecho de la Universidad de la República e é professora na Facultad de Ingeniería de la Universidad de Montevideo em direito informático e proteção de dados pessoais. Além disso, ensina direito e novas tecnologias na Licenciatura de Dados para Negócios da Universidad de Montevideo. Membro ativo da

Ordem dos Advogados do Uruguai e membro fundadora do Instituto de Direito Informático da Faculdade de Direito da Universidade da República, tem participado de diversos grupos de trabalho na área (Rede Iberoamericana de Proteção de Dados, Grupo de Berlim, Rede Acadêmica Internacional de Proteção de Dados Pessoais e Assuntos Afins, International Association of Privacy Professionals, entre outros) e foi designada Embaixadora do *privacy by design*. Foi assessora jurídica do Parlamento Nacional, atendendo questões do Senado e da Câmara dos Deputados de seu país de 1992 a 2019, onde contribuiu ativamente com vários legisladores para a aprovação da lei uruguaia de proteção de dados pessoais em 2008.

Jonathan Mendoza Iserte

Doutor em Direito e Mestre em Regulamento Geral de Proteção de Dados da União Europeia. Atualmente, atua como Secretário de Proteção de Dados Pessoais no Instituto Nacional de Transparência, Acesso à Informação e Proteção de Dados Pessoais (INAI) do México, onde tem trabalhado em padrões da indústria, diretrizes governamentais e promovido colaborações público-privadas em termos de privacidade e gestão de dados. Dr. Mendoza é especialista em Proteção de Dados Pessoais, Privacidade, Tecnologias Disruptivas e Ética Digital, o que o levou a palestrar em diversos fóruns nacionais e internacionais sobre privacidade e proteção de dados pessoais. Ele possui 50 publicações como autor e coautor sobre direitos humanos, proteção de dados pessoais, privacidade, inteligência artificial e neurodireitos. Além disso, possui ampla trajetória acadêmica, destacando sua participação como professor convidado e de disciplina em diversas universidades públicas e privadas do México, integrando o corpo docente do Mestrado em Regulamento Geral de Proteção de Dados da União Europeia, do Diploma de Proteção de Dados Pessoais da Escola Livre de Direito e diversos programas acadêmicos em países latino-americanos como Argentina e Panamá.

Pablo Andrés Palazzi

Professor de Direito na Universidade de San Andrés (UDESA). Professor visitante da Fundação Getulio Vargas (RJ, Brasil) e da Fordham Law School (NYC, EUA). Diretor acadêmico do Centro de Tecnologia e Sociedade (CETyS) da Universidade de San Andrés. Especialista em direito da Internet, proteção de dados, crimes cibernéticos, privacidade, propriedade intelectual, liberdade de expressão e acesso à informação. É editor da revista latino-americana de proteção de dados pessoais e diretor da publicação "Proteção de Dados: Doutrina e Jurisprudência" (CDYT 2020-2025), editada pelo CETyS da Universidade de San Andrés. É diretor do Diploma Internacional em Proteção de Dados Pessoais da UDESA. Em 2000, recebeu o prêmio da Agência Espanhola de Proteção de Dados por seu trabalho em matéria de transferência internacional, e em 2021 recebeu o *Vanguard Award* da Associação Internacional de Profissionais de Privacidade (IAPP, em inglês) por suas contribuições ao desenvolvimento da privacidade na América Latina. Sócio da Allende & Brea (Buenos Aires, Argentina).

Nelson Remolina Angarita

Professor Associado da Faculdade de Direito da Universidade dos Andes (Bogotá, Colômbia). Doutor *Summa Cum Laude* em Ciências Jurídicas pela Pontifícia Universidade Javeriana. Mestre em Direito pela London School of Economics and Political Science. Especialista em Direito Comercial e Advogado pela Universidade dos Andes. Cofundador (2001) e diretor do GECTI - Grupo de Estudos em Internet, Comércio Eletrônico, Telecomunicações & Informática (Disponível em: http://gecti.uniandes.edu.co/) da Faculdade de Direito da Universidade dos Andes. Fundador (2008) e diretor do Observatório Ciro Angarita Barón sobre a Proteção de Dados Pessoais na Colômbia (Disponível em:). Sua obra sobre Coleta Internacional de Dados Pessoais recebeu o prêmio da Agência Espanhola de Proteção de Dados (AEPD) por sua contribuição à América Latina. Foi Superintendente Delegado para a Proteção de Dados Pessoais (outubro de 2018 a março de 2022) da Superintendência de Indústria e Comércio da República da Colômbia (autoridade colombiana de proteção de dados). Autor de diversas publicações sobre tratamento de dados pessoais, neurotecnologias, neurodireitos, neurodados, ciberespaço, comércio eletrônico, títulos e valores eletrônicos, alternativas de identificação eletrônica, entre outros temas.

Agradecimentos

Esta obra foi revisada por pares. Os autores agradecem particularmente os professores doutores Filipe Medon, Matías Mascitti, e Bianca Kremer e os pesquisadores Walter B. Gaspar, Fernando Naegele e Daniel Dore Lage pelos valiosos comentários e sugestões sobre as versões preliminares deste trabalho.

Este trabalho foi desenvolvido no âmbito do projeto Data Regulations, generosamente patrocinado pela Open Society Foundations (OSF) e executado pelo Centro de Tecnologia e Sociedade da FGV DIREITO RIO. Os autores agradecem sinceramente o apoio da OSF e da FGV DIREITO RIO, sem o qual esta obra não teria sido possível.

Dedicatória

Os autores dedicam este trabalho à memória do professor Danilo Doneda (1970-2022), um excelente parceiro intelectual e um amigo querido sem o qual os autores não se teriam encontrado.

Abreviações

AAIP | Agencia de Acceso a la Información Pública (Argentina)

ANPD | Autoridade Nacional de Proteção de Dados (Brasil)

ANPD | Autoridad Nacional de Protección de Datos (Peru)

AWS | Amazon Web Services

BCR | Binding Corporate Rules (Normas Corporativas Vinculantes)

CADH | Convenção Americana sobre Direitos Humanos

CBPR | Cross Border Privacy Rules (Sistema de regras de privacidade transfronteiriças)

CE | Comissão Europeia

CIPDP | Comissão Interamericana para a Proteção de Dados Pessoais

CONVENIO 108 | Convenção para a Proteção das Pessoas no que diz respeito ao Tratamento Automatizado de Dados Pessoais (Conselho da Europa, 1981)

CONVENIO 108+ | Versão modernizada da Convenção para a Proteção das Pessoas no que diz respeito ao Tratamento Automatizado de Dados Pessoais (Conselho da Europa, 2018)

CtIDH | Corte Interamericana de Direitos Humanos

DNPDP | Dirección Nacional de Protección de Datos Personales (Argentina)

EEE | Espaço Econômico Europeu

EDPB | European Data Protection Board (Conselho Europeu de Proteção de Dados)

EPDP | Normas de Proteção de Dados Pessoais (da Rede Ibero-Americana de Proteção de Dados)

GDPR | General Data Protection Regulation (Regulamento Geral de Proteção de Dados da União Europeia)

INAI | Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (México)

LFPDPPP | Ley Federal de Protección de Datos Personales en Posesión de Particulares (México)

LGPDPPSO | Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (México)

LGPD | Lei Geral de Proteção de Dados Pessoais (Brasil)

NAPD | Nível Adequado de Proteção de Dados Pessoais

NCG | Normas Corporativas Globais

PEN | Poder Executivo Nacional (Argentina)

RIPD | Rede Ibero-Americana de Proteção de Dados

SCC | Standard Contractual Clauses (Cláusulas Contratuais Modelo ou Cláusulas-Padrão Contratuais)

SIC | Superintendencia de Industria y Comercio (Colômbia)

TIDP | Transferência Internacional de Dados Pessoais

TJUE | Tribunal de Justiça da União Europeia

UE | União Europeia

URCDP | Unidad Reguladora y de Control de Datos Personales (Uruguai)

WP29 | Working Party Art. 29 (Grupo de Trabalho do Artigo 29 da União Europeia)

Sumário

Introdução

1 Transferências de dados na América Latina: entre a fragmentação e a interoperabilidade legislativa

Este livro tem como objetivo proporcionar uma análise inicial do complexo, embora convergente, panorama das transferências de dados pessoais na América Latina, lançando luz sobre os desafios em evolução, as respostas regulatórias e as possíveis soluções compartilhadas que podem moldar este aspecto crucial da governança de dados em nível regional.

Apesar das semelhanças normativas e regulatórias existentes, não tem sido fácil para os países latino-americanos construírem um quadro regional que permita promover fluxos livres e seguros de dados pessoais e formar uma abordagem e uma visão comuns para a governança de dados.

A maior parte da América Latina já adotou marcos nacionais de proteção de dados muito semelhantes na maioria de seus elementos devido ao uso do modelo europeu como fonte comum de inspiração. Também vale a pena notar que a Rede Ibero-Americana de Proteção de Dados tem servido até agora como um centro unificador para muitas ideias na região.

Além disso, a Corte Interamericana de Direitos Humanos (CtIDH) reconheceu expressamente, em outubro de 2023, a autodeterminação informativa como um direito humano autônomo de respeito e cumprimento obrigatórios no sistema interamericano de direitos humanos.

De fato, na Sentença Série C nº 506 de 18 de outubro de 2023, a CtIDH concluiu:

> 586. Na opinião da Corte Interamericana, os elementos precedentes dão origem a **um direito humano autônomo: o direito à autodeterminação informativa**, reconhecido em diversos ordenamentos jurídicos da região, e que está incluído no conteúdo protetivo da Convenção Americana, em particular com base nos direitos conti-

> dos nos artigos 11 e 13, e, na dimensão de sua proteção jurisdicional, no direito garantido pelo artigo 25".[1]
>
> (…)
>
> 588. Em suma, **trata-se de um direito autônomo que serve, por sua vez, de garantia de outros direitos**, como os relativos à vida privada, à proteção da honra, à salvaguarda da reputação e, em geral, à dignidade da pessoa. Ressalte-se que o direito abrange, com as limitações aplicáveis (infra parágrafos 601 a 608), **quaisquer dados de natureza pessoal em posse de qualquer órgão público, e também opera com relação a registros ou bases de dados mantidas por pessoas físicas**, questões que não são aprofundadas devido à finalidade deste processo internacional"[2](enfatizamos)

Trata-se de uma decisão icônica, de enorme relevância no sistema interamericano de direitos humanos, porque, dentre outras coisas, impõe deveres aos Estados e abre as portas para que sejam garantidos pelos tribunais internacionais de justiça.

A adoção de mecanismos para garantir a prática (não no papel ou na teoria) é precisamente um dos deveres que os Estados devem cumprir, como pode ser visto a partir do seguinte enfatizado pela CtIDH:

> 599. De qualquer forma, a Corte Interamericana reitera que **a efetividade do direito à autodeterminação informativa exige que os Estados prevejam mecanismos ou procedimentos adequados, ágeis, livres e eficazes para tramitar e responder aos procedimentos, seja pela mesma autoridade que administra os dados ou por outra instituição competente em matéria de proteção ou supervisão de dados pessoais** (par. 582 supra) 755, (...) **Este requisito, derivado do dever estabelecido no artigo 2 da Convenção Americana**, na medida em que engloba a emissão de normas e o desenvolvimento de práticas conducentes à observância dos direitos humanos, incluindo procedimentos administrativos apropriados, constitui uma garantia essencial para fazer valer e exercer o direito [3] (Destaque)

---

1 Cf. *Sentença da Corte Interamericana de Direitos Humanos* de 18 de outubro de 2023. Série C nº 506. O texto oficial da sentença disponível em: https://jurisprudencia.corteidh.or.cr/vid/953775991

2 Cf. *Sentença da Corte Interamericana de Direitos Humanos* de 18 de outubro de 2023. Série C nº 506. O texto oficial da sentença disponível em: https://jurisprudencia.corteidh.or.cr/vid/953775991.

3 Cf. *Sentença da Corte Interamericana de Direitos Humanos* de 18 de outubro de 2023. Série C nº 506. O texto oficial da sentença disponível em: https://jurisprudencia.corteidh.or.cr/vid/953775991.

Pretende-se aproveitar a oportunidade histórica para a região, partindo de uma análise pragmática de alguns dos sistemas mais proeminentes do continente e, assim, apresentar algumas propostas ambiciosas sobre como a América Latina poderia construir seu futuro em termos de proteção de dados.

No campo da proteção de dados pessoais, uma questão que tem sido fundamental para promover o desenvolvimento e a adoção de regulamentos nesta área são as transferências internacionais de dados, que são de grande importância hoje devido à globalização e à natureza cada vez mais interconectada de nossa sociedade.

Muitos países latino-americanos adotaram a abordagem europeia de proteção de dados na esperança de se tornarem um "porto seguro" onde os dados seriam enviados livremente da Europa. No entanto, é relevante refletir se estamos fazendo o mesmo para que as informações exportadas da América Latina sejam protegidas e tratadas adequadamente, a fim de garantir os direitos dos latino-americanos com relação aos seus dados pessoais e direitos relacionados (bom nome, devido processo, liberdade, privacidade, entre outros).

Em um mundo cada vez mais digital, empresas e organizações precisam transferir constantemente dados pessoais entre diferentes países e regiões para realizar suas atividades e operações diárias. A importância das transferências internacionais de dados pessoais reside em vários aspectos, um deles é o comércio internacional, pois permitem que as empresas transfiram informações sobre produtos, serviços, pagamentos e outros aspectos comerciais a nível global.

Por outro lado, as transferências internacionais de dados são cruciais para a pesquisa e desenvolvimento em diversos campos, como ciência, tecnologia, inteligência artificial e medicina, pois permitem que os pesquisadores compartilhem dados e informações para avançar em suas pesquisas.

As transferências internacionais de dados pessoais também representam desafios em termos de privacidade e segurança da informação. Portanto, marcos regulatórios, mecanismos e acordos internacionais foram estabelecidos para garantir a proteção de dados pessoais e a privacidade dos indivíduos no contexto das transferências internacionais de dados. Um dos mecanismos mais conhecidos é a decisão de adequação emitida por uma autoridade, procedimento que avalia se o nível de proteção ofe-

recido pela legislação do país ou região importadora de dados pessoais é equivalente ao do exportador.

Um exemplo disso é o processo de adequação para países terceiros à União Europeia, o que, do lado latino-americano, só foi concluído pela Argentina e pelo Uruguai, sendo que a Colômbia e o México estão no processo. Processos de adequação também foram iniciados entre os países latino-americanos. Por exemplo, a Colômbia fez esse pedido frente ao Uruguai e à Argentina. Ainda não há decisão sobre esta questão por ambos os países.

Esse mecanismo não é o único existente e, atualmente, mais de setenta países criaram regulamentos de transferência de dados, adotando critérios extremamente heterogêneos[4]. Em todo o mundo, iniciou-se um debate em torno da regulação das transferências internacionais entre os blocos econômicos existentes para além da União Europeia, como os BRICS, formado por Brasil, Rússia, Índia, China e África do Sul, e recentemente ampliado.[5] Da mesma forma, a discussão atingiu o mais alto nível e o tema foi colocado nas agendas dos países mais ricos do G7, formado por Alemanha, Canadá, Estados Unidos da América, França, Itália, Japão e Reino Unido, e da OCDE, onde se multiplicam as iniciativas dedicadas ao chamado "Livre fluxo de dados com confiança".[6]

---

4 Ver CHANDER, Anupam e SCHWARTZ, Paul M., Privacidade e/ou Comércio. *Revisão de Direito da Universidade de Chicago,* n. 49, 2023. p. 90.

5 BELLI, Luca; DONEDA, Danilo. Proteção de Dados nos Países do BRICS: Interoperabilidade Jurídica por meio de Práticas Inovadoras e Convergência. Lei Internacional de Privacidade de Dados. *Imprensa da Universidade de Oxford*, v. 13, p. 1-24, 2023.

6 O conceito de *Data Free Flow with Trust* (DFFT) foi introduzido pela primeira vez pelo ex-presidente do Japão, Shinzo Abe, na reunião do Fórum Econômico Mundial de 2019. O conceito de DFFT afirma que garantir a confiança em termos de privacidade, segurança e direitos de propriedade intelectual é um pré-requisito para o livre fluxo de dados através das fronteiras. O conceito foi endossado em junho de 2019 por membros do grupo de nações do G20. Veja G20. "Declaração dos Líderes do G20 em Osaka". (29 de junho de 2019). Sob a presidência japonesa de 2023, a Cúpula do G7 em Hiroshima endossou a "Visão dos Ministros de Tecnologia e Digital do G7 para operacionalizar o livre fluxo de dados com confiança e suas prioridades", incluindo o estabelecimento de um "Acordo de Parceria Institucional". Veja G7. Declaração Ministerial - A Reunião dos Ministros Digitais e de Tecnologia do G7. (30/04/2023).
Nesse contexto, a Declaração de Ministros de Tecnologia e Digital do G7 afirmou ainda que "os atributos da OCDE e seu trabalho atual nas áreas de governança de dados, privacidade, livre fluxo de dados com confiança e economia digital a tornam adequada para avançar nesse esforço internacional" Ver G7. Anexo 1 da trilha digital e tecnológica - *Visão do G7 para operacionalizar o DFFT e suas prioridades*. (30/04/2023).

2 Evoluções e desafios

O rápido avanço das tecnologias digitais transformou a forma como os dados pessoais são coletados, tratados e transferidos através das fronteiras, apresentando oportunidades e desafios para indivíduos, empresas, pesquisadores e governos em todo o mundo.

No contexto latino-americano, a dinâmica das transferências de dados pessoais é influenciada por uma infinidade de fatores, incluindo dimensões históricas, culturais, legais, econômicas e tecnológicas. Nesse contexto, nas últimas décadas, a América Latina passou por vários estágios de desenvolvimento sociopolítico, econômico e legislativo, cada um dos quais deixou sua marca na abordagem da região em relação às transferências de dados pessoais.

Das experiências ditatoriais do século XX à globalização moderna, embora marcada por legados coloniais, o fluxo de informações foi submetido a mudanças nas dinâmicas de poder, marcos legais, normas sociais e evolução dos modelos de negócios. O passado colonial da região, marcado por práticas extrativistas e concentração de riqueza, se reflete claramente na moderna mineração de dados, que lançou as bases para fluxos de dados assimétricos, muitas vezes priorizando os interesses de atores externos sobre os das populações locais.[7]

Nesse contexto, os avanços legislativos das duas primeiras décadas do século XXI representaram avanços saudáveis e positivos, embora a eficácia dos marcos regulatórios latino-americanos ainda seja bastante limitada.

Na segunda metade do século XX, a América Latina testemunhou uma onda de regimes autoritários, caracterizados por vigilância e censuras generalizadas, que complicaram ainda mais o cenário da proteção e transferência de dados pessoais e o pleno gozo dos direitos fundamentais.

---

7 Ver por exemplo QUIJANO, Aníbal. 2000. Colonialidade do poder e eurocentrismo na América Latina. *Sociologia Internacional*, v. 15, n. 2, p. 215-232. 2000; AVILA PINTO, Renata. ¿Soberanía digital o colonialismo digital? *Revista Internacional de Direitos Humanos*, v. 15, n. 27, p. 15-28. 2018. RICAURTE, P. Epistemologias de dados, a colonialidade do poder e a resistência. *Televisão e Novas Mídias*, v. 20, n. 4, 350-365. 2019; COULDRY, Nick, MEJIAS, Ulises A. 2019. Colonialismo de dados: repensando a relação da big data com o assunto contemporâneo. *Televisão e Novas Mídias*, v. 20, n. 4. p. 336-49. 2019; MORALES, E.; REILLY, K. *Subordinado pelo algoritmo: explorando o colonialismo de dados entre cidadãos latino-americanos.* AoIR selecionou artigos de pesquisa na Internet. 2023.

A luta pela democracia e pelos direitos humanos na região tem alimentado o debate sobre a importância do direito fundamental à privacidade e de um direito autônomo à proteção de dados, estimulando o surgimento de marcos legais voltados para a salvaguarda desses direitos. A partir da concepção do direito ao *habeas data*, foram lançadas as bases para a consagração do direito fundamental à proteção de dados na região, tornando mais transparentes os poderes público e privado.

Nada obstante, a chegada da internet e das tecnologias digitais trouxe novos desafios, como a necessidade de transparência e proteção não apenas contra o uso abusivo pelos governos no exercício da soberania estatal, mas também contra os abusos de novos soberanos privados que operam transnacionalmente e cujas fronteiras digitais ocupam espaços transnacionais, desafiando as noções tradicionais de jurisdição e controle.[8] Nesse contexto, o debate em torno da regulação das transferências de dados é fundamental para facilitar a cooperação internacional e, ao mesmo tempo, fortalecer a soberania digital do Estado, ou seja, a capacidade de "exercer agência, poder e controle para moldar a infraestrutura, os dados, os serviços e os protocolos digitais".[9] através daquilo que um número crescente de acadêmicos define como "soberania de dados".[10]

Hoje, a América Latina está em uma encruzilhada, lutando com as complexidades das transferências de dados pessoais em meio à rápida

8 Ver por exemplo BELLI, L. O poder estrutural como elemento crítico da soberania privada das plataformas digitais. Em CELESTE, E., HELDT, A. e IGLESIAS KELLER, C. (Ed). *Constitucionalizando as mídias sociais*, p. 81-100. Oxford: Publicação Hart. 2022; ZUBOFF, S. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder.* Nova York: Relações Públicas. 2019; OESTE S. Capitalismo de dados: redefinindo as lógicas de vigilância e privacidade. *Negócios e Sociedade*, v. 58, n. 1, p. 20-41, 2017.

9 Neste sentido, ver JIANG, M.; BELLI, L. (Ed.). *Soberania digital dos países do BRICS: como o Sul Global e as alianças de poder emergentes estão remodelando a governança digital.* Cambridge: Cambridge University Press. 2024; BELLI, L. "Construindo um bom soberano digital por meio de infraestruturas públicas digitais e bens comuns digitais na Índia e no Brasil", Think20 (T20) do G20. (2023). Disponível em: https://tinyurl.com/2fyvf298.

10 A soberania de dados pode ser definida como "a capacidade de entender como e por que os dados (pessoais) são processados e por quem, desenvolver recursos de tratamento de dados e regular efetivamente o tratamento de dados, mantendo assim a autodeterminação e o controle". Ver BELLI, L.; GASPAR W.; JASWANT S. Soberania de dados e transferências de dados como elementos fundamentais da transformação digital: lições dos países do BRICS. *Revisão da Lei e Segurança da Computação*. Edição especial - Transformação Digital nos Países do BRICS. 2024. Disponível em: https://www.sciencedirect.com/special-issue/10VRL9GGMQG.

inovação tecnológica e interconexão global. Por um lado, a proliferação de plataformas digitais, computação em nuvem, comércio eletrônico, *Big Data* e inteligência artificial facilitou e depende em grande parte dos fluxos de dados transfronteiriços. Esses fluxos estão se tornando cada vez mais essenciais para o crescimento econômico e a inovação. Por outro lado, as preocupações com proteção de dados, privacidade, segurança cibernética e vigilância aumentaram os apelos por uma supervisão regulatória mais rígida, cooperação internacional e padrões harmonizados capazes de proteger efetivamente os indivíduos e garantir o Estado de Direito.

Nesse contexto, formuladores de políticas, juristas e partes interessadas do setor se envolvem em discussões contínuas sobre o equilíbrio apropriado entre os direitos dos titulares dos dados, os imperativos econômicos e as necessidades democráticas. Desde as revelações do ex-funcionário da Agência de Segurança Nacional dos EUA, Edward Snowden, e o caso Facebook-Cambridge Analytica, vários escândalos destacaram os perigos de não ter uma estrutura robusta de proteção de dados, levando os países latino-americanos a adotar, reavaliar e melhorar seus regimes de proteção de dados.

Por outro lado, a falta de regulação do fenômeno da coleta internacional de dados pessoais na América Latina[11] cria um vácuo muito grande na região, especialmente quando muitas das regulações atuais não têm aplicação extraterritorial, como ocorre com o regime da União Europeia e das leis mais modernas. As regras relativas às transferências internacionais foram concebidas sob o pressuposto de que os dados são enviados de um país para outro(s) país(es). Em outras palavras, os dados são exportados do país de origem para o país de destino. Todavia, não se pensou sobre o que fazer quando os dados dos cidadãos de um país não são exportados ou enviados, mas são coletados de outro(s) país(es). Este último é o que chamamos de coleta internacional de dados, um fenômeno que ainda está ausente dos regulamentos de tratamento de dados. Acreditamos que atualmente mais dados saem de um país por meio da coleta internacional do que da trans-

11 REMOLINA, Nelson. *Recolha internacional de dados pessoais: um desafio do mundo pós-internet*, edição do Diário Oficial do Estado, pp 245. 2015. (Prêmio Ibero-Americano de Proteção de Dados de Pesquisa 2014).

ferência internacional de dados. É por isso que também é importante agir sobre o fenômeno da coleta internacional de dados.[12]

O modelo europeu, refinado desde a Convenção 108 do Conselho da Europa até o mais recente Regulamento Geral de Proteção de Dados (GDPR), ganhou destaque e influência internacional, tornando-se uma fonte de inspiração para todos os países latino-americanos.[13]

No entanto, apesar deste óbvio "efeito Bruxelas",[14] o cenário regional permanece fragmentado, apesar de todos os quadros existentes terem sido claramente baseados nas diferentes versões do modelo europeu. Nesse contexto, o objetivo dos autores deste livro é explorar as dimensões multifacetadas das transferências de dados pessoais na América Latina, examinando uma seleção dos marcos regulatórios mais proeminentes da região, identificando semelhanças e diferenças e lançando luz sobre quais estratégias podem simplificar esse cenário complexo, encontrando um novo caminho latino-americano.

3 Complexidade, oportunidades e o "tropicalismo" dos dados pessoais

Devido à sua fonte comum de inspiração, a maioria das estruturas de proteção de dados latino-americanas compartilha semelhanças relevantes, mas também algumas pequenas grandes diferenças, devido como e quando o modelo europeu foi integrado e adaptado às especificidades locais. Essa complexidade fica evidente ao nos aprofundarmos nos desafios da transferência internacional de dados pessoais.

De fato, esse cenário complexo costuma ser moldado por um número significativo de fatores jurídicos, técnicos, econômicos, jurídicos e sociopo-

12 REMOLINA, Nelson. *Recolha internacional de dados pessoais: um desafio do mundo pós-internet*, edição do Diário Oficial do Estado, pp 245. 2015. (Prêmio Ibero-Americano de Proteção de Dados de Pesquisa 2014).

13 Ver, por exemplo, CARRILLO, Arturo J.; JACKSON, Matías. (2022). Seguir o líder? Um estudo de direito comparado do impacto do Regulamento Geral de Proteção de Dados da UE na América Latina. 16 *Viena J. Int'l Const*. L. 177. págs. 177-262. 2022.

14 Ver BRADFORD, Anu. *O Efeito Bruxelas: Como a União Europeia governa o mundo*. Oxford: Oxford University Press. 2020.

líticos, e a América Latina não está isenta de uma dinâmica tão complexa. Em particular, a América Latina enfrenta vários desafios importantes em termos de fragmentação jurídica, questões jurisdicionais transfronteiriças, segurança de dados e capacidade de aplicação da lei muito limitada, devido a recursos e maturidade institucional muitas vezes muito limitados.

No que diz respeito à fragmentação jurídica e à possibilidade de harmonização, é importante notar que, apesar de muitas semelhanças e de um passado colonial comum, a América Latina não goza de uma organização supranacional específica, capaz de harmonizar ações da mesma forma que a União Europeia. As opções existentes têm diferentes níveis de alcance geográfico, normativo e político, que vão desde o Mercado Comum do Sul (MERCOSUL), mais limitado geograficamente, até a Organização dos Estados Americanos (OEA), passando pela União de Nações Sul-Americanas (UNASUL) e pela Comunidade Andina de Nações (CAN).

Todos esses fóruns oferecem um lugar interessante para discutir como melhorar a cooperação regional em termos de governança de dados e alguns deles já iniciaram uma conversa embrionária sobre isso, como a OEA,[15] o MERCOSUL[16] e a CAN.[17] Esses espaços podem ser explorados

15 Como a própria OEA aponta, desde 1996 a Organização é responsável pela proteção de dados pessoais por meio de seus órgãos. O site da OEA lembra que "a Assembleia Geral da OEA vem aprovando resoluções sobre o assunto, instando os Estados-membros a tomar certas ações e, às vezes, conferindo mandatos específicos a outros órgãos da Organização. O tema também esteve na agenda da Comissão Jurídica Interamericana (CJI), que em 2000 apresentou o documento "O Direito à Informação: Acesso e Proteção da Informação e Dados Pessoais em Formato Eletrônico". Desde aquele ano, o CJI continuou a trabalhar nesta área. Em particular, em 2012, a CJI aprovou uma "Proposta de Declaração de Princípios sobre Privacidade e Proteção de Dados Pessoais nas Américas"; em 2015, o "Guia Legislativo sobre Privacidade e Proteção de Dados Pessoais nas Américas" e em 2021, os "Princípios Atualizados sobre Privacidade e Proteção de Dados Pessoais, com Anotações", buscando contribuir para o desenvolvimento de um marco para salvaguardar, nos países das Américas, os direitos das pessoas físicas à proteção de seus dados pessoais e à autodeterminação em matéria de informação". Disponível em: https://www.oas.org/es/sla/ddi/proteccion_datos_personales.asp.

16 Veja MERCOSUL. Medidas de Proteção de Dados Pessoais e sua Livre Circulação. *MERCOSUL/CMC/P. DEC. N° 10/04.* Mercosul Bloco de tradimento. 2010.

17 A Decisão Andina 897 de 14 de julho de 2022 da Comunidade Andina de Nações (CAN) substituiu a Decisão 638 da Comunidade Andina de Nações (CAN) sobre as Diretrizes para a Proteção dos Direitos dos Usuários de Serviços de Telecomunicações. Pela primeira vez, foi incluído um capítulo sobre o tratamento de dados pessoais (Capítulo II. Proteção dos direitos dos usuários no que diz respeito à propriedade, tratamento e circulação de dados pessoais). Esta Decisão é muito importante, porque pela primeira vez em nível andino esta

para superar a fragmentação das estruturas legais que regem a proteção de dados e a privacidade, que resulta em uma inconsistência frustrante em toda a região, apesar das fortes semelhanças das estruturas existentes.

No entanto, os autores estão mais do que cientes da dificuldade em chegar a acordos no campo das organizações intergovernamentais e, nesse sentido, o segundo capítulo deste livro analisa como as transferências de dados poderiam ser facilitadas por meio de cláusulas-padrão contratuais, uma opção recentemente proposta pela Rede Ibero-Americana de Proteção de Dados.[18] Nesse sentido, um dos principais objetivos deste livro é explorar estratégias que possam facilitar a convergência e reduzir as disparidades no nível de proteção dos dados pessoais das pessoas na região. De fato, a fragmentação legal existente complica, aumenta custos e reduz os benefícios potenciais para todo o espectro de partes interessadas, pesquisadores, governos e, especialmente, empresas.

A complexidade e a inevitabilidade das questões jurisdicionais transfronteiriças são maximizadas pela natureza sem fronteiras da Internet, o que facilita muito os intercâmbios, ao mesmo tempo em que levanta questões sobre como regular efetivamente as transferências de dados transfronteiriças. Em particular, os países latino-americanos – como todos os países com estruturas nacionais de proteção de dados – muitas vezes podem enfrentar conflitos jurisdicionais quando os dados são transferidos de e para jurisdições com padrões legais e mecanismos de aplicação divergentes e sobrepostos. Como resultado, garantir a conformidade legal e proteger os

questão é regulamentada e esta norma obrigatória, imediata e supranacional impacta países que ainda não possuem regulamentação sobre proteção de dados pessoais (Bolívia). Nesse sentido, esse país, assim como Colômbia, Equador e Peru, também "reconhece e garante o direito de todos os usuários da Comunidade Andina ao tratamento adequado de seus dados pessoais e à propriedade sobre eles, bem como o direito de acesso, uso, retificação, eliminação, cancelamento, oposição, limitação ao tratamento ou circulação dos mesmos e à portabilidade de suas informações". Além disso, são estabelecidos os seguintes princípios que devem ser observados no tratamento de tais informações: "legalidade; lealdade; Legitimação; transparência; propósito; Proporcionalidade; qualidade, veracidade e precisão; segurança; confidencialidade e responsabilidade demonstrada" (CAN. *Artigo 4.º da Decisão Andina 897 de 2022*. Comunidade Andina de Nações. 2022).

18 Rede Ibero-Americana de Proteção de Dados. *Guia de Implementação de Cláusulas Contratuais Modelo para a Transferência Internacional de Dados Pessoais (TIPD).* Rede Ibero-Americana. 2023. Disponível em: https://www.redipd.org/es/documentos/guiasx.

direitos dos indivíduos no contexto das transferências internacionais de dados torna-se cada vez mais complexo.

Uma das razões para essa complexidade são as diferentes maneiras pelas quais a segurança dos dados é garantida em diferentes países. As transferências internacionais de dados acarretam riscos inerentes à segurança e privacidade dos dados e, em geral, à perda de controle sobre seus dados e à autodeterminação informacional dos titulares dos dados, que é a própria essência dos marcos de proteção de dados. Essa preocupação é particularmente relevante em países com níveis muito diferentes de desenvolvimento tecnológico, prontidão para segurança cibernética, maturidade e eficácia institucional. Assim, os países latino-americanos muitas vezes sofrem com uma notável escassez de recursos e conhecimentos necessários para definir e monitorar a implementação de diretrizes de segurança de dados pessoais e mitigar efetivamente o risco de violações de dados, ataques cibernéticos ou simples má gestão de dados durante transferências internacionais de dados.[19]

Esses desafios são maximizados pela capacidade muito limitada de aplicação da lei que caracteriza as autoridades latino-americanas de proteção de dados. Na verdade, a maioria dos países latino-americanos luta com recursos e capacidade de aplicação muito desafiadores para cumprir efetivamente as leis de proteção de dados e regular as transferências internacionais de dados. Essa falta de capacidade de cumprimento prejudica a eficácia dos regulamentos existentes e pode levar a lacunas e inconsistências consideráveis em termos de aplicação, particularmente no contexto de transferências internacionais de dados.

Claramente, as operações de transferência de dados podem envolver uma gama incrivelmente ampla de riscos que expõem dados pessoais a acesso não autorizado, uso indevido ou perda. A superação desses desafios requer abordagens holísticas e pragmáticas que permitam identificar todo o espectro de soluções potenciais para promover a convergência e o progresso colaborativo. Este livro se esforça para seguir esse caminho, fornecendo uma análise do cenário atual e propondo algumas soluções inovadoras. De fato, os autores deste volume acreditam que a situação atual, embora apresente muitos desafios, também oferece oportunidades únicas

19 BELLI, Luca; DONEDA, Danilo. O que falta ao Brasil e à América Latina para uma proteção de dados efetiva? *Revista JOTA de Privacidad*, 2 sep. 2021. Disponível em: http://bit.ly/3xAujH7.

de progresso. Nunca na história os marcos de proteção de dados foram tão abundantes e semelhantes na região e há uma clara vontade política de cooperar, desde que isso possa trazer progresso e benefícios compartilhados para todos os parceiros latino-americanos.

É importante ressaltar que as reflexões contidas neste volume foram nutridas e amadurecidas ao longo de vários anos de debates, com um papel particularmente relevante desempenhado pela CPDP LatAm, a conferência sobre Computadores, Privacidade e Proteção de Dados na América Latina,[20] como um local fundamental para a troca de ideias, pesquisas e debates multissetoriais e propostas de políticas. A conferência fornece um exemplo revelador de porque o diálogo e a cooperação multissetorial em nível regional podem ser muito úteis na identificação de problemas compartilhados, propondo soluções e construindo redes de pessoas com ideias semelhantes, interessadas em tentar implementar tal proposta em benefício da região.

Os autores deste livro têm interagido, trocado ideias, construído amizades e se engajado em discussões intelectualmente estimulantes desde o início da CPDP LatAm, e estão particularmente conscientes da importância de ter uma plataforma estável que permita o debate livre, a identificação de problemas e novas ideias ousadas. De fato, uma versão embrionária deste volume foi apresentada pela primeira vez para comentários na CPDP LatAm 2023, cujo tema principal foi "Proteção de Dados, Cooperação e Inovação na América Latina".[21]

Em virtude dessa experiência prática de pesquisa e diálogo *multissetorial*, os autores não só tiveram a possibilidade de fortalecer seu trabalho graças aos comentários e sugestões de amigos e colegas, mas também testaram o interesse que as propostas de políticas voltadas para a convergência regional poderiam ter. É interessante notar que a grande maioria das partes interessadas que participaram das discussões sobre como melhorar a cooperação em nível regional concorda que o compartilhamento de

20 Disponível em: www.cpdp.lat.

21 Veja BELLI, Luca; BRIAN NOUGÈRES Ana; MENDOZA ISERTE Jonathan; PALAZZI, Pablo A.; REMOLINA ANGARITA, Nelson. *Rumo a um modelo latino-americano de adequação para a transferência internacional de dados pessoais*. Documento de discussão apresentado na Conferência de Computadores, Privacidade e Proteção de Dados da América Latina (CPDP LatAm) 2023 para comentários. Disponível em: https://cpdp.lat/wp-content/uploads/2023/07/doc-discusion-cpdplatam23-2.3.pdf.

padrões e mecanismos de cooperação seria muito benéfico para todos os atores da região, seja no setor público, privado ou científico. Nesse contexto, é bastante surpreendente que, apesar de já existirem catorze marcos nacionais de proteção de dados muito semelhantes, nenhum país latino-americano tenha pensado em propor tal cooperação.

A esse respeito, é útil notar que a iniciativa mais avançada para promover fluxos regionais de dados veio da Rede Ibero-Americana de Proteção de Dados, que propôs as Cláusulas-padrão contratuais que exploramos no segundo capítulo deste volume.[22] Embora esta iniciativa seja extremamente valiosa, é interessante notar que a Rede foi criada através de, e ainda tem, forte tração ibérica, mais do que latino-americana.[23] Por que a América Latina não pode desenvolver seu próprio sistema de proteção de dados pessoais sem a necessidade de uma liderança europeia? A região perdeu a confiança em si mesma? Ou talvez nunca a tenha encontrado? Não é do interesse da América Latina influenciar o debate internacional e criar um modelo consistente com sua tradição e necessidades? Um dos objetivos fundamentais deste trabalho é injetar otimismo e confiança na região, promovendo a pesquisa local, o pensamento doutrinário e a inovação das políticas latino-americanas, apoiando fortemente o surgimento de uma nova corrente de pensamento sobre proteção de dados, que poderíamos definir como "Tropicalismo de Proteção de Dados".

A América Latina deve adotar uma abordagem multifacetada que combine inovações regulatórias e tecnológicas e promova a cooperação internacional. Portanto, este trabalho visa lançar as bases para um esforço colaborativo renovado entre acadêmicos, organizações da sociedade civil, governos e reguladores da região, empresas e organizações internacionais, para facilitar o desenvolvimento de padrões harmonizados de proteção de dados, promover mecanismos de cooperação transfronteiriça e melhorar a confiança dos indivíduos no ecossistema digital regional.

A evolução histórica da proteção de dados na América Latina está intimamente ligada à trajetória mais ampla da região de consolidação democrática, defesa dos direitos humanos, reforma legal e avanço tecnológico.

---

22 Rede Ibero-Americana de Proteção de Dados. *Cláusulas contratuais modelo***.** Rede Ibero-Americana. 2023. Disponível em: https://www.redipd.org/es/documentos/guias.

23 Nesse sentido, veja Carrillo e Jackson. 2022.; Bradford. 2020., já referido.

Com este livro, os autores pretendem oferecer elementos importantes para reflexão, que permitirão abordar esses desafios das transferências de dados de forma proativa. Assim, estamos convencidos de que os países latino-americanos podem definir suas próprias soluções para aproveitar os benefícios das tecnologias digitais e do tratamento de dados, salvaguardando os direitos individuais e coletivos e promovendo a governança responsável de dados em um mundo cada vez mais interconectado.

4 Como entender este livro?

A evolução histórica da proteção de dados na América Latina reflete uma complexa interação de princípios constitucionais, obrigações internacionais, marcos legislativos, decisões regulatórias e esforços colaborativos destinados a propor soluções inovadoras para salvaguardar os direitos dos titulares dos dados e promover sua governança responsável. Construindo sobre estas bases e enfrentando os desafios existentes, os países latino-americanos podem continuar avançando em direção a uma estrutura de proteção de dados mais robusta e harmonizada, estimulando a convergência nacional e defendendo os direitos e liberdades fundamentais por meio de padrões homogêneos.

É certo que a exploração das opções disponíveis para facilitar as transferências de dados revela uma variedade de mecanismos concebidos para garantir o cumprimento das normas de proteção de dados, permitindo simultaneamente o fluxo regulado de dados pessoais através das fronteiras. Este volume não pretende ser exaustivo, mas pretende proporcionar ao leitor uma compreensão de quais são os modelos mais proeminentes adotados no contexto latino-americano e quais são as opções disponíveis para promover a interoperabilidade jurídica entre os sistemas da região.[24]

24 A interoperabilidade é geralmente descrita como "a capacidade de transferir e gerar dados úteis e outras informações entre sistemas, aplicativos ou componentes". Veja União Internacional de Telecomunicações. *Documento de Discussão GSR: Interoperabilidade no Ecossistema Digital*. União Internacional de Telecomunicações, Genebra, Suíça. 2015. Portanto, a interoperabilidade é a propriedade que permite a troca e o uso de informações entre tecnologias e sistemas heterogêneos. Esse conceito está se tornando cada vez mais importante à medida que as tecnologias interconectadas, que recebem e transmitem dados continuamente, estão se tornando a norma. Do ponto de vista técnico, a interoperabilidade é promovida através da adoção de normas e protocolos técnicos partilhados que permitem a todos os utilizadores da Internet trocar informações e utilizar serviços além-fronteiras. O conceito de interoperabilidade tem

Desde a década de 1990, um menu cada vez maior de opções regulatórias foi criado para disciplinar os fluxos internacionais de dados. Esses mecanismos incluem decisões de adequação, cláusulas-padrão contratuais ou cláusulas contratuais específicas, regras corporativas vinculantes, obrigações internacionais decorrentes de acordos multilaterais e bilaterais, regulamentos setoriais e códigos de conduta.

Como discutimos neste volume, cada país normalmente adota sua própria combinação especial das opções acima mencionadas, temperada com requisitos regulatórios específicos que geralmente diferem de país para país, apesar de surgirem de uma base comum de princípios. Os cinco modelos nacionais que exploramos, a saber, Argentina, Brasil, Colômbia, México e Uruguai, apresentam peculiaridades interessantes. No primeiro capítulo deste livro, analisamos o regime de transferência de dados de cada país, com atenção especial à forma como eles regulam:

- **Decisões de adequação**, que implicam o reconhecimento pela autoridade nacional de proteção de dados de que um país terceiro, território ou organização internacional assegura um nível adequado de proteção de dados comparável às normas

sido associado a diferentes benefícios, incentivando a abertura e influenciando positivamente a concorrência e a inovação, ao mesmo tempo em que aumenta a eficiência no fornecimento de uma maior diversidade de conteúdos e serviços. A interoperabilidade também está associada a reduções no custo das tecnologias, pois promove a escalabilidade. Benefícios semelhantes podem ser alcançados promovendo a interoperabilidade de uma perspectiva regulatória (ou seja, por meio da interoperabilidade jurídica) em vez de uma perspectiva exclusivamente técnica. Nessa perspectiva, a interoperabilidade jurídica é a propriedade de promover a compatibilidade de normas relativas ao mesmo assunto em diferentes jurisdições ou diferentes níveis administrativos dentro de um Estado. Tal como a interoperabilidade técnica, a interoperabilidade jurídica estimula o intercâmbio de informações no âmbito de diferentes sistemas. Como tal, a interoperabilidade dos sistemas técnicos e jurídicos permite que os indivíduos (e, em particular, os utilizadores da Internet) acedam e prestem serviços além-fronteiras e beneficiem de igual proteção dos direitos em diferentes sistemas, graças a regras, princípios, normas e procedimentos compatíveis (ou comuns). As regras e os princípios partilhados entre vários sistemas jurídicos têm o potencial de reduzir os custos de transação, esvaziar os obstáculos ao comércio transfronteiriço e promover benefícios não mensuráveis, como a proteção dos direitos fundamentais; Ver BELLI, Luca e DONEDA, Danilo. 2023, citado acima, nota 2; ROLF WEBER. A interoperabilidade jurídica como instrumento de combate à fragmentação. *Série de Documentos da Comissão Mundial sobre a Governação da Internet* (4). 2014; BELLI, Luca e ZINGALES, Nicolo. Interoperabilidade para promover ecossistemas digitais abertos nos BRICS. *Relatório da Conferência Mundial da Internet*. Academia Chinesa de Estudos do Ciberespaço. 2023.

nacionais. Essa opção é uma das mais difundidas em todo o mundo, mas ao mesmo tempo criticada pela necessidade de um processo burocrático consideravelmente complexo e muitas vezes politicamente sensível.

- **Cláusulas Contratuais Modelo**, também conhecidas como cláusulas-padrão contratuais (SCCs), que são acordos contratuais pré-aprovados desenvolvidos por autoridades reguladoras para regular a transferência de dados pessoais. Ao incorporar essas cláusulas aos acordos de transferência de dados, as partes podem demonstrar seu compromisso em proteger os direitos dos titulares dos dados e mitigar os riscos associados às transferências internacionais de dados. Essas ferramentas são reconhecidas por sua flexibilidade e praticidade e o segundo capítulo deste livro explora um experimento muito recente e inovador liderado pela Rede Ibero-Americana de Proteção de Dados, que consiste na criação de cláusulas-padrão contratuais ibero-americanas.
- **Regras** corporativas vinculantes, que as empresas multinacionais geralmente incluem em suas políticas internas para enquadrar as regras de governança de dados. Essas ferramentas de regulação privada devem ser aprovadas pelas autoridades de proteção de dados para serem consideradas válidas, permitindo a transferência de dados pessoais dentro de organizações multinacionais ou grupos de empresas, garantindo consistência e responsabilidade entre diferentes jurisdições.
- **Códigos de conduta e certificações**, que podem ser aceitos pelas legislações nacionais como regulações válidas para setores específicos, fornecendo orientações e salvaguardas adicionais para transferências internacionais de dados. Por exemplo, setores como saúde, finanças e telecomunicações podem ter requisitos regulatórios específicos ou mecanismos de autorregulação que regem a transferência transfronteiriça de dados pessoais sensíveis.
- **Os acordos internacionais** entre países também podem facilitar as transferências de dados, estabelecendo o reconheci-

> mento mútuo de padrões de proteção de dados, facilitando a cooperação institucional – por exemplo, entre agências reguladoras – em fluxos de dados transfronteiriços, até mesmo a inclusão de cláusulas que estabelecem o livre fluxo de dados por padrão entre as partes.

O segundo e o terceiro capítulos deste livro adotam uma postura mais proativa e exploram soluções que poderiam ser adotadas por reguladores e governos da região para facilitar as transferências de dados com confiança. O segundo capítulo explora o modelo de cláusulas contratuais desenvolvido pela Rede Ibero-Americana de Proteção de Dados, analisando o conceito e as vantagens das cláusulas e enfatizando a consistência desse instrumento regulatório com as normas ibero-americanas existentes.

Por fim, o terceiro capítulo deste volume se aventura na discussão sobre como poderia ser uma Convenção Latino-Americana de Proteção de Dados e quais seriam os benefícios de promover tal abordagem. A maioria dos princípios, direitos e obrigações incluídos nesta proposta são destilados de estruturas legislativas existentes na região, mas a proposta também inclui elementos aspiracionais que ainda não estão explicitamente contidos na legislação existente, como, por exemplo, a necessidade de a proteção de dados ser aplicada às atividades *de enforcement da lei* e o acesso aos dados por órgãos governamentais.

É importante destacar que os elementos que compõem a proposta da Convenção Latino-Americana sobre Proteção de Dados também podem ser utilizados como base para a construção de um *checklist* que facilite o processo de adaptação em nível regional, estimulando assim a interoperabilidade regulatória por meio de uma abordagem baseada em *soft law*.

Por fim, é importante observar que as opções identificadas acima não representam necessariamente uma lista exaustiva de todas as estratégias possíveis para facilitar os fluxos de dados com confiança. Por exemplo, uma opção que ainda não foi explorada em nível latino-americano, mas que vem sendo experimentada com sucesso na Índia há vários anos, é o gerenciamento de dados por meio *de software*.[25] Esta opção, apesar de ser

25 Em particular, o sistema indiano promove o uso de um tipo de infraestrutura pública digital chamada "Arquitetura de Capacitação e Proteção de Dados", cujo objetivo é gerenciar o

particularmente interessante e promissora, ainda não é explorada neste trabalho, mas será objeto de pesquisas futuras.

Nosso trabalho também enfatiza que, em geral, a disponibilidade e a eficácia desses mecanismos para facilitar as transferências de dados na América Latina dependem de vários fatores, incluindo o cenário legal e regulatório, e a capacidade institucional e política em cada momento para fornecer cooperação regional. Certamente, a América Latina enfrenta um conjunto único de desafios e oportunidades em termos de transferências de dados, apesar de ter estruturas nacionais de proteção de dados muito semelhantes.

Portanto, a esperança dos autores deste livro é que nossa pesquisa possa promover um debate muito necessário sobre como construir uma maior integração na proteção de dados no nível latino-americano, oferecendo algumas ideias concretas sobre como isso poderia acontecer na prática.

Também é possível pensar que as ideias propostas neste artigo poderiam inspirar um esforço para desenvolver uma estrutura regional de proteção de dados, por um grupo limitado de países latino-americanos com interesses semelhantes e sistemas jurídicos compatíveis, sem a necessidade de depender de uma organização intergovernamental pré-existente. Portanto, podemos pensar que um esforço plurilateral liderado por um pequeno grupo de países abertos à colaboração com todos os Estados latino-americanos pode ser considerado uma opção potencialmente bem-sucedida.

Por fim, queremos reconhecer que uma versão preliminar do capítulo I deste artigo foi apresentada na Computers Privacy and Data Protection Conference Latin America 2023 (CPDP LatAm) no Rio de Janeiro, Brasil, a fim de receber *feedback* dos participantes do evento[26]. Esses comentários foram consolidados na versão final deste artigo e os autores agradecem as valiosas contribuições recebidas da comunidade da CPDP LatAm. A versão corrigida com comentários foi publicada na obra coletiva Proteção de

consentimento para o tratamento de dados. Veja BELLI, Luca e DONEDA, Danilo. Proteção de Dados nos Países do BRICS: Interoperabilidade Jurídica por meio de Práticas Inovadoras e Convergência. pág. 18-20. 2023. cit. supra; Para uma perspectiva crítica sobre o modelo indiano de infraestrutura pública digital, consulte Parsheera, S. Stack is the New Black?: Evolution and Outcomes of the 'India-Stackification' Process. *Revisão de Lei e Segurança de Computadores*. v. 52, abril 2024. Disponível em: https://doi.org/10.1016/j.clsr.2024.105947.

26 Ver **Computers Privacy and Data Protection Conference Latin America.** Disponível em: https://cpdp.lat/pt-br/programa/.

Dados Pessoais: Doutrina e Jurisprudência, volume 4 (Pablo Palazzi, compilador), Buenos Aires, Argentina. Essa versão foi premiada pelo *Future of Privacy Forum* com o "*Privacy Papers for Policymakers Award*".

Queremos também reconhecer que uma versão preliminar do projeto de Convenção Interamericana sobre Autodeterminação, Tratamento e Circulação de Dados Pessoais Informativos, incluída no anexo ao Capítulo III deste trabalho, foi apresentada na conferência CPDP LatAm 2024, a fim de receber comentários. O feedback que recebemos foi particularmente valioso para melhorar o texto inicial e os autores agradecem aos participantes da CPDP LatAm por seu apoio.

Luca Belli
Rio de Janeiro, Brasil

Ana Brian Nougrères
Montevidéu, Uruguai

Jonathan Mendoza Iserte
Cidade do México, México

Pablo Andrés Palazzi
Buenos Aires, Argentina

Nelson Remolina
Bogotá, Colômbia

Julho de 2024.

Capítulo 1
As Regras Vigentes e a Necessidade de se Desenvolver um Modelo Latino-Americano de Adequação para a Transferência Internacional de Dados Pessoais

Introdução

No âmbito da proteção de dados pessoais, um tema que tem sido fundamental para impulsionar o desenvolvimento e a adoção de regulamentações nessa área é o das transferências internacionais de dados, que são de grande importância atualmente, devido à globalização e à natureza cada vez mais interconectada de nossa sociedade. Em um mundo cada vez mais digital, empresas e organizações precisam transferir dados pessoais constantemente entre diferentes países e regiões para realizar suas atividades e operações diárias.

A importância das transferências internacionais de dados pessoais reside em vários aspectos, sendo um deles o comércio internacional, pois as transferências permitem que as empresas transmitam informações sobre produtos, serviços, pagamentos e outros aspectos comerciais em escala global. Ademais, como destacamos anteriormente, as transferências internacionais de dados são cruciais para a pesquisa e o desenvolvimento de diversos setores, como a ciência, a tecnologia – incluindo sistemas de inteligência artificial – e a medicina.

As transferências internacionais de dados pessoais também apresentam desafios em termos de privacidade e segurança da informação. Por isso, foram estabelecidos marcos regulatórios, mecanismos e acordos internacionais para garantir a proteção dos dados pessoais e a privacidade dos indivíduos no contexto das transferências internacionais de dados. Um dos mecanismos mais conhecidos é o procedimento de adequação de países destinatários da transferência, conforme a legislação do país ou região em questão.

Este mecanismo não é o único atual: ao redor do mundo, iniciou-se um debate em torno da regulamentação das transferências internacionais nos blocos econômicos existentes, como o composto por Brasil, Rússia, Índia, China e África do Sul, mais conhecido como BRICS[27]. Da mesma forma, a discussão chegou ao nível mais alto, sendo o tema incluído nas agendas dos países mais ricos do G7, composto por Alemanha, Canadá, Estados Unidos, França, Itália, Japão e Reino Unido.

1 Justificativa

Os especialistas em privacidade e proteção de dados pessoais dos países latino-americanos perceberam que a transformação digital é um elemento essencial para o futuro de suas economias e sociedades. Sob essa perspectiva, a proteção de dados se torna uma prioridade para fomentar ambientes digitais prósperos, nos quais as pessoas desfrutam de proteções e as empresas se beneficiam da segurança jurídica e do livre fluxo de dados pessoais.

Dado o notável valor econômico e estratégico que os dados pessoais adquiriram, a regulamentação dessa "nova classe de ativos"[28] também se torna um fator essencial para a afirmação da soberania digital. Nos últimos cinco anos, a necessidade urgente de regulamentar os dados pessoais estimulou a proposta, adoção e implementação de regulamentos de proteção de dados pessoais cada vez mais compatíveis entre si.

Assim, nasceu na região latino-americana uma iniciativa de implementar um modelo latino-americano de adequação, para garantir o livre fluxo de dados pessoais entre os países da região, tomando como ponto de partida os processos de adequação vigentes no mundo. Por sua localização geográfica, o continente americano se torna um ponto de encontro entre os cinco continentes, de modo que estabelecer um padrão comum facilita o tratamento e o fluxo de dados pessoais, em um exercício que be-

27 BELLI, Luca; DONEDA, Danilo. "Data Protection in the BRICS Countries: Legal Interoperability through Innovative Practices and Convergence". *International Data Privacy Law*. Oxford University Press, v. 13, n. 1, p. 1-24, fev. 2023. Disponível em: https://doi.org/10.1093/idpl/ipac019.

28 World Economic Forum. *Personal Data: The Emergence of a New Asset Class*. Janeiro de 2011. Disponível em: https://bit.ly/3SpCbU3.; The Economist. *The world's most valuable resource is no longer oil, but data*, 6 maio 2017. Disponível em: https://bit.ly/3MxqIy5.

neficiará todos os envolvidos, como os desenvolvedores, o setor privado e o usuário final dos produtos e serviços oferecidos.

2 Alcance do capítulo

Esta parte da obra é focada em alguns dos países que integram a região latino-americana. Esperamos que a proposta sirva de orientação e guia para as autoridades de proteção de dados pessoais da região e forneça as bases para elaborar um instrumento pelo qual se estabeleça um padrão comum para a garantia e a salvaguarda dos dados pessoais nas transferências transfronteiriças de dados pessoais e, ao mesmo tempo, assegure o livre fluxo de dados pessoais na região.

Os objetivos deste capítulo são:

- Identificar os aspectos comuns e as diferenças existentes nas regras de transferências internacionais de dados pessoais dos países latino-americanos;
- Determinar se essas regras são suficientes para garantir o devido tratamento dos dados dos titulares que são transferidos para outros países;
- propor ferramentas e mecanismos comuns para facilitar o livre fluxo de dados pessoais, sempre garantindo o nível de proteção dos direitos dos titulares cujos dados são transferidos dos países analisados para outros países do mundo;
- propor alternativas para melhorar o nível de proteção dos direitos dos titulares cujos dados são transferidos dos países analisados para outros países do mundo;
- propor mecanismos de proteção dos direitos dos titulares cujos dados são coletados de outros países (coleta internacional de dados).

3 Metodologia

Nosso objetivo com este trabalho é estabelecer as bases para um modelo latino-americano de adequação que, como outros exercícios existentes não apenas na região, mas também em nível internacional, segue os parâmetros necessários para oferecer confiabilidade e segurança ao tratamento de dados pessoais.

Os países que fizerem parte desse modelo deverão integrar os antecedentes normativos que regulam a proteção de dados pessoais em suas respectivas jurisdições e enfatizar a regulamentação emitida quanto ao tratamento de dados pessoais em transferências nacionais e internacionais, se for o caso. Além disso, se a regulamentação de seu país estabelecer um procedimento de adequação para outros países, deverá indicar o procedimento implementado ou, se o país em questão já foi aprovado como país adequado em um processo de adequação, indicar a experiência e os requisitos que teve que cumprir para tal aprovação.

Quanto ao procedimento para adotar um ato de execução relativo à adequação da proteção de dados pessoais, esse será iniciado com uma análise exaustiva do ordenamento jurídico do país destinatário, especificamente de sua legislação na matéria e de sua aplicação prática em casos concretos em que os direitos dos titulares de dados pessoais foram discutidos.

De maneira específica, são avaliados, entre outros, os seguintes aspectos:

- A estrutura jurídica das normas de dados pessoais e seu âmbito de aplicação material e pessoal;
- Os compromissos internacionais assumidos pelo país destinatário, bem como as obrigações decorrentes de sua participação em sistemas multilaterais ou regionais, particularmente em relação à defesa dos direitos humanos, da privacidade e da proteção de dados pessoais, e o cumprimento dessas obrigações;
- Os direitos dos titulares: acesso, retificação, cancelamento, oposição e portabilidade;
- Os deveres e obrigações dos controladores e operadores do tratamento, incluindo a observância obrigatória dos princípios de proteção de dados pessoais reconhecidos internacionalmente;

- As limitações para realizar transferências de dados pessoais posteriormente;
- As medidas de supervisão do cumprimento das normas, incluindo a existência de uma autoridade de controle independente encarregada de fiscalizar e fazer cumprir as regras em matéria de proteção de dados. Essa autoridade deve atuar com total independência e imparcialidade no desempenho de suas funções e no exercício de suas competências;
- A existência de recursos administrativos e ações judiciais eficazes, incluindo a indenização por danos e prejuízos, que possam ser exercidos pelo titular quando seu direito for violado ou por ações ou omissões por parte da autoridade de controle;
- A existência de salvaguardas específicas para o tratamento de dados pessoais no contexto de ações judiciais e penais, de segurança nacional, entre outros casos específicos.

Este compêndio é um primeiro exercício de aproximação, para conhecer o estado da arte em relação à regulamentação vigente em matéria de transferências de dados pessoais. Uma vez finalizado este primeiro exercício, serão determinados mecanismos adicionais que facilitem a disseminação e promoção do modelo na região.

Nos próximos pontos, analisaremos, um a um, os sistemas de transferências internacionais na Argentina, Brasil, Colômbia, México e Uruguai (em ordem alfabética). Esta análise servirá de base para entender como funciona atualmente o sistema legal de cada um dos países mencionados, e, a partir daí, buscar elementos comuns que permitam desenvolver um modelo latino-americano de adequação.

4 Argentina

4.1 Introdução ao sistema argentino

A Lei de Proteção de Dados Pessoais nº 25.326 foi aprovada no ano de 2000. Sua regulamentação, por meio do Decreto nº 1.558, foi aprovada em 2001.

A República da Argentina foi declarada um país adequado pela União Europeia em 30 de junho de 2003.[29] A Argentina ratificou a Convenção 108 e a Convenção 108 modernizada (Convenção 108+).

4.2 Regras sobre transferência internacional e exceções

O artigo 12.1 da Lei de Proteção de Dados Pessoais proíbe a transferência de dados pessoais de qualquer tipo para países que não proporcionem níveis de proteção adequados. Essa lei não define o que implica proporcionar "níveis de proteção adequados".

De acordo com o artigo 12.2 da referida norma, a proibição não se aplicará em alguns casos, que são:

a) Colaboração judicial internacional;
b) Intercâmbio de dados de caráter médico, quando assim o exigir o tratamento do afetado ou uma investigação epidemiológica;
c) Transferências bancárias ou de valores mobiliários, no que se refere às respectivas transações e conforme a legislação aplicável;
d) Quando a transferência for acordada no âmbito de tratados internacionais dos quais a Argentina seja parte; e
e) Quando a transferência tiver como objetivo a cooperação internacional entre organismos de inteligência para o combate ao crime organizado, terrorismo e narcotráfico.

A lei argentina contemplou exceções limitadas devido à importância do tema. O decreto regulamentar as ampliou, inspirando-se naquelas previstas no artigo 26 da então vigente Diretiva Europeia de Proteção de Dados de 1995, o que resultou em uma maior harmonização com o regime europeu.

Ademais, razões lógicas levaram à conclusão de que a Argentina não poderia se isolar em um mundo interconectado, sendo necessário adotar salvaguardas, como medidas contratuais, para permitir a continuidade

29 UNIÃO EUROPEIA. *Decisión de la Comisión, del 30 de junio de 2003, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina*, União Europeia, Diario Oficial, n. L 168, p. 19, 5 jul. 2003. Disponível em: bit.ly/3Oue6mz.

das transferências existentes entre empresas de um mesmo grupo econômico ou entre controladora e controladas.

O decreto regulamentar (artigo 12, Decreto nº 1.558/2001) estabelece que a proibição de transferir dados pessoais para países ou organismos internacionais ou supranacionais que não proporcionem níveis de proteção adequados não se aplica quando o titular dos dados tiver consentido expressamente a cessão.

O decreto regulamentar da Lei de Proteção de Dados Pessoais também acrescenta que:

> Não é necessário o consentimento no caso de transferência de dados de um registro público que esteja legalmente constituído para facilitar a informação ao público e que esteja aberto à consulta do público em geral ou de qualquer pessoa que possa demonstrar um interesse legítimo, desde que sejam cumpridas, em cada caso particular, as condições legais e regulamentares para a consulta (artigo 12 do Decreto nº 1.558/2001).

Finalmente, seguindo a Diretiva Europeia (artigo 26), o artigo 12 do decreto regulamentar permite que as partes que transferem dados internacionalmente para países não adequados recorram a contratos ou cláusulas que assegurem uma proteção adequada. Apesar de o Decreto nº 1.558/2001 autorizar o uso de cláusulas contratuais para transferir dados pessoais para jurisdições com leis "não adequadas", até o ano de 2016, a Direção Nacional de Proteção de Dados Pessoais (DNPDP) não manifestou quais países tinham leis adequadas nem aprovou um modelo oficial de contrato de transferência internacional.

4.3 A disposição 60/2016 sobre adequação e cláusulas-padrão contratuais

Tudo isso mudou quando a agência de dados pessoais da Argentina, por meio da Disposição 60/2016[30], fez o seguinte:

30 Para uma análise completa da norma citada, ver: PALAZZI, Pablo. Las transferencias internacionales de datos personales en el anteproyecto de ley de protección de datos personales. *Revista Latinoamericana de Protección de Datos Personales*, n. 4, 2018.

- Aprovou dois contratos modelo para a transferência de dados pessoais para países não adequados;
- Regulamentou a necessidade de solicitar autorização para usar um modelo diferente do oficial;
- Determinou uma lista de países "adequados" ao sistema argentino de proteção de dados pessoais;
- Deixou a "porta aberta" para continuar incluindo novos países na "lista branca" de países aprovados.

Como se pode observar, a agência argentina de dados pessoais, em um único ato normativo, fez duas coisas importantes: elaborou uma lista de países adequados e aprovou modelos de contratos para transferência internacional de dados pessoais.

Antes da Disposição nº 60/2016, não era necessário obter aprovação prévia da DNPDP. Também não existia um modelo de contrato padrão aprovado pela autoridade reguladora argentina, como ocorria na Europa com as cláusulas contratuais padrão.

Os controladores e operadores do tratamento eram livres para elaborar contratos de transferência internacional sem um guia específico da DNPDP ou aprovação prévia. Embora não houvesse aprovação prévia, a DNPDP podia, a pedido da parte interessada, analisar rascunhos de contratos e emitir um parecer sobre sua adequação, caso o controlador do tratamento optasse por apresentá-lo. Esses pareceres formaram um corpo de jurisprudência administrativa que permitia interpretar os requisitos para estabelecer uma base legal para a transferência internacional de proteção de dados pessoais para uma jurisdição não adequada.

Na prática, os controladores e operadores do tratamento usavam um modelo que seguia de perto o aprovado na União Europeia, como se podia concluir dos pareceres da DNPDP, que sugeriam modificações nos contratos submetidos ou aprovavam o documento apresentado para autorização com pequenas mudanças, referentes à citação da legislação local em vez da europeia.

4.4 Determinação de países adequados na disposição 60/2016

A finalidade da Disposição n. 60/2016 é "garantir um nível adequado de proteção de dados pessoais nos termos do artigo 12 da Lei 25.326 naquelas transferências de dados que tenham como destino países sem legislação adequada". De acordo com o artigo 1º da Disposição nº 60/2016, os modelos devem ser usados "naquelas transferências de dados que tenham como destino países sem legislação adequada". Se o país de destino tiver uma legislação adequada (de acordo com a DNPDP), então não devem ser utilizados modelos contratuais nem qualquer contrato. Tudo isso sem prejuízo de que as partes sejam livres para regulamentar a transferência com um contrato genérico de tratamento de dados, de locação de serviços ou um genérico de *outsourcing* (cumprindo os requisitos do artigo 25 da lei e do decreto). Esta decisão dá suporte à liberdade das partes de não usar contratos de transferência quando esta ocorre para países da União Europeia (ou reconhecidos pela UE como adequados), onde a legislação obviamente é adequada, pois a União Europeia é o modelo da lei argentina.

4.5 Quais são os países adequados de acordo com a autoridade argentina?

O artigo 3º da Disposição n. 60/2016 estabelece que, para fins de aplicação da presente disposição, consideram-se países com legislação adequada: Estados-membros da União Europeia e membros do Espaço Econômico Europeu (EEE), Suíça, Guernsey, Jersey, Ilha de Man, Ilhas Faroé, Canadá (apenas em relação ao seu setor privado), Andorra, Nova Zelândia, Uruguai e Israel (apenas em relação aos dados que recebem um tratamento automatizado).

Com esta lista "positiva" de países, a Argentina adota um modelo semelhante de "lista branca" sem mencioná-lo explicitamente, ou seja, autoriza transferências para países considerados adequados pela UE. Adota-se este sistema, mas sem aderir formalmente ou estritamente à UE. As conclusões semelhantes às da UE fazem sentido, pois a Argentina segue o modelo europeu de proteção de dados pessoais. No entanto, isso também

implica, de certa forma, delegar uma função soberana a outro país (a de reconhecer um país como adequado).

Conforme indicam os Considerandos da Disposição n. 60, em um processo que tramitou na DNPDP, o Ministério da Justiça analisou a legislação daqueles países classificados como tendo legislação adequada pela União Europeia e concluiu sobre o nível equivalente das normativas desses países em relação à lei argentina de proteção de dados. O processo mencionado é um estudo realizado pela DNPDP (quando estava sob a tutela do Ministério da Justiça e antes de ser transferida para a Agência de Acesso à Informação Pública – AAIP) em 2012, que estabeleceu essa lista. No entanto, a lista não é fechada, pois a agência argentina poderia, de ofício ou a pedido de partes interessadas, realizar análises sobre outros países ou organismos internacionais.

É por isso que a norma esclarece que a "enumeração (de países adequados) será revisada periodicamente por esta Direção Nacional, publicando a lista e suas atualizações em seu site oficial na Internet". Essa atualização pode servir para incluir novos países adequados ou para retirar da lista alguns países que não oferecem garantias adequadas para manter a adequação.

O Reino Unido, após sua saída da União Europeia (Brexit), teve que ser reavaliado como um terceiro país para ver se era "adequado". Apesar de não estar na UE, se mantivesse sua infraestrutura legislativa e uma agência independente de proteção de dados, poderia continuar sendo um país adequado para fins de transferência de dados pessoais. A UE acabou declarando o Reino Unido como país adequado em 28 de junho de 2021.

No entanto, a Argentina, já em 2019, modificou a Disposição 60 através da Resolução AAIP 34/2019 e incluiu o Reino Unido como país adequado, a pedido do próprio Reino Unido[31], apresentado quando o Brexit já havia sido votado e era uma realidade, mas a saída formal do Reino Unido da UE ainda estava pendente.

Os Considerandos da Resolução AAIP 34/2019 manifestam o seguinte:

> Que foi recebida uma solicitação por parte do DEPARTAMENTO DE SERVIÇOS DIGITAIS, CULTURA, MÍDIA E ESPORTE DO REINO UNIDO DA GRÃ-BRETANHA E IRLANDA DO NORTE, requerendo que a AGÊNCIA DE ACESSO À INFORMAÇÃO PÚ-

31 Na Argentina, os "considerandos" são uma forma de transferir para uma decisão administrativa um raciocínio jurídico onde se justificam ou explicam os fundamentos da decisão.

> BLICA adote as medidas necessárias para garantir que o fluxo internacional de dados pessoais da REPÚBLICA ARGENTINA para o REINO UNIDO DA GRÃ-BRETANHA E IRLANDA DO NORTE continue de maneira ininterrupta após a saída do REINO UNIDO DA GRÃ-BRETANHA E IRLANDA DO NORTE da UNIÃO EUROPEIA. Que, de acordo com o informado na respectiva solicitação e em conformidade com a revisão de antecedentes por parte da AGÊNCIA DE ACESSO À INFORMAÇÃO PÚBLICA, os padrões de proteção de dados pessoais fornecidos pelo REINO UNIDO DA GRÃ-BRETANHA E IRLANDA DO NORTE foram mantidos e até reforçados em comparação com a situação normativa do Estado solicitante no momento em que a então DIREÇÃO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS decidiu incluir os Estados-membros da UNIÃO EUROPEIA — incluindo o REINO UNIDO DA GRÃ-BRETANHA E IRLANDA DO NORTE — na lista de países com legislação adequada (artigo 3 da Disposição 60 - E/2016). Que, pelos motivos expostos, a AGÊNCIA DE ACESSO À INFORMAÇÃO PÚBLICA considera que o REINO UNIDO DA GRÃ-BRETANHA E IRLANDA DO NORTE continua fornecendo um nível de proteção adequado nos termos da Lei nº 25.326.

Os Estados Unidos não estão mencionados na "w*hite list*" da DNPDP porque, na prática, a DNPDP da Argentina sempre considerou que o país não possui uma lei geral de proteção de dados como os demais países europeus, nem uma agência independente de proteção de dados (a FTC é independente, mas se dedica ao direito do consumidor, não a dados pessoais). Também não são mencionados países latino-americanos que tinham leis de proteção de dados sólidas na data da normativa (2016), como México ou Colômbia, exceto o Uruguai, que foi declarado um país adequado pela Comissão Europeia alguns anos antes da Disposição nº 60.[32]

O modelo contratual aprovado pela Disposição 60/2016 deve ser usado pelas partes que transferem dados. Caso não utilizem o modelo, devem solicitar autorização à DNPDP. O pedido de autorização deve ser feito até trinta dias após a assinatura do contrato. No entanto, nada impede o pedido que seja apresentado antes desses trinta dias, ou até mesmo sem ter assinado o contrato.

32 PALAZZI, Pablo. Las transferencias internacionales de datos personales en el anteproyecto de ley de protección de datos personales. *Revista Latinoamericana de Protección de Datos Personales*, n. 4, 2018.

Essa previsão surge do artigo 2º da Disposição 60/2016, que estabelece: "aqueles controladores do tratamento que efetuem transferências de dados pessoais para países que não possuam legislação adequada nos termos do artigo 12 da Lei nº 25.326 e seu Decreto Regulamentar nº 1.558/01, e utilizem contratos que diferem dos modelos aprovados no artigo anterior ou não contenham os princípios, garantias e conteúdos relativos à proteção dos dados pessoais previstos nos modelos aprovados, deverão solicitar sua aprovação a esta Direção Nacional apresentando-os, no máximo, dentro de trinta (30) dias corridos de sua assinatura".

Entendemos que este reconhecimento de adequação realizado pela DNPDP não se estende automaticamente a organizações que utilizam *binding corporate rules* (BCR) ou que implementaram cláusulas-padrão contratuais seguindo o modelo europeu para as transferências internacionais. O reconhecimento de adequação aplica-se às jurisdições mencionadas no artigo 3º e visa evitar a necessidade de ter um acordo ao transferir dados exclusivamente para essas jurisdições.

Se uma organização estiver transferindo dados pessoais com base em um modelo anterior não aprovado ou homologado pela DNPDP, ou com base em outras vias como as *binding corporate rules* (BCR), deverá cumprir a Disposição 60/2016. As BCR são um conjunto de regras ou cláusulas corporativas vinculantes que têm por objetivo estabelecer as práticas que uma organização realiza em matéria de tratamento de dados pessoais para facilitar as transferências internacionais de dados no seio dessa entidade. Constituem um instrumento que os grupos multinacionais podem utilizar perante as autoridades de proteção de dados para garantir a legalidade das operações de transferência de dados em sua organização, independentemente de o país de destino assegurar ou não um "nível adequado de proteção" conforme a normativa vigente no país de origem dos dados. As BCR foram reconhecidas na Argentina pela Resolução n. 159/2018 da AAIP. Nestes casos, o mais prudente seria submeter o contrato à autorização ou utilizar o modelo contratual aprovado.

Na Argentina, a partir da Disposição n. 60/2016, existe um "modelo oficial" de contrato aprovado pela DNPDP, que segue as diretrizes das cláusulas-padrão vigentes na Europa em 2018. De fato, o artigo 1º da Disposição 60/2016 as denomina "cláusulas contratuais padrão", e os Considerandos da

Disposição 60 as indicam como fonte da norma. Falta que a Argentina atualize essas cláusulas-padrão para as aprovadas pela UE em 2021.

A Disposição DNPDP 60 aprovou dois modelos:

i. Um para transferência internacional de dados para outro controlador; um caso típico é a matriz que centraliza dados das subsidiárias locais; e
ii. O outro modelo é para a prestação de serviços, que pode ser com a matriz ou com um terceiro que fornece serviços e que, logicamente, está fora do país (se não, não haveria transferência internacional).

A leitura das cláusulas do contrato modelo permite inferir que o contrato possui certos elementos essenciais destinados a oferecer um nível adequado de proteção na transferência e que devem estar presentes nos contratos que se afastam do modelo. Esses elementos mínimos são:

- Referência à Lei nº 25.326, ao definir os conceitos de dados pessoais, dados sensíveis, tratamento, controlador e titular do dado;
- Identificação da autoridade ou órgão de controle da Argentina;
- Referência ao artigo 25 da Lei nº 25.326 ao mencionar o importador ou o operador, no modelo de contrato de transferência internacional para a prestação de serviços;
- Definir a legislação de proteção de dados como a Lei nº 25.326 e normativa regulamentar;
- Detalhar a finalidade e a classe de dados pessoais que são transferidos;
- Estabelecer certas obrigações mínimas para o importador, ou seja, quem recebe os dados. Essas obrigações mínimas incluem: medidas de segurança, cumprimento do princípio da finalidade, estabelecer uma pessoa de contato dentro da organização do importador, permitir auditorias ou inspeções por um auditor independente ou até mesmo pela autoridade de controle, notificar pedidos de cessão de autoridades estrangeiras ou acessos não autorizados, atender aos pedidos de di-

reito de acesso, destruir os dados após o término do contrato ou cumprida a finalidade, manter um registro das obrigações assumidas e, o mais importante: tratar os dados pessoais de acordo com a Lei de Proteção de Dados Pessoais nº 25.326;

- Solidariedade entre ambas as partes: cada uma das partes deverá responder perante os titulares dos dados pelos danos que lhes causaram como resultado da violação de direitos reconhecidos no contrato de transferência, nos termos previstos pela Lei nº 25.326, suas normas regulamentares e direito de fundo da Argentina. Isso pode dar origem a reclamações de responsabilidade civil extracontratual, administrativa, sancionatória ou até mesmo contratual. Por exemplo, a cláusula 5ª do modelo aprovado pela DNPDP diz que "Nos casos em que se alegue descumprimento por parte do importador de dados, o titular do dado poderá solicitar ao exportador que tome as medidas apropriadas para cessar esse descumprimento";
- Cláusula sobre terceiros beneficiários: ambos os modelos de contrato contêm uma cláusula sobre terceiros beneficiários ou *third party beneficiary*. Por meio dessa cláusula, os titulares dos dados poderão exigir do importador (com quem não têm relação direta), na qualidade de terceiros beneficiários, o cumprimento das disposições da Lei nº 25.326 relacionadas ao tratamento de seus dados pessoais;
- Lei aplicável e jurisdição: estabelece a lei argentina e a autoridade de controle; mesmo no caso de terceiros beneficiários, o importador submete-se à jurisdição argentina, tanto na esfera judicial quanto administrativa (isso é a jurisdição administrativa da DNPDP). Essa cláusula é imposta em virtude da previsão de ordem pública da norma (artigo 44, Lei nº 25.326);
- Resolução do contrato: caso o importador de dados não cumpra as obrigações que lhe são cabíveis em virtude das cláusulas-padrão da DNPDP, o exportador de dados deverá suspender temporariamente a transferência de dados pessoais ao importador até que o descumprimento seja sanado. Além disso, o contrato será considerado resolvido, em caso de sus-

pensão superior a trinta dias, por descumprimento da lei, ou por decisão da DNPDP que estabeleça que o importador ou o exportador de dados não cumpriram a Lei nº 25.326 ou os princípios consagrados no contrato; e

- O modelo de contrato para prestação de serviço contém uma cláusula adicional relativa ao subtratamento (*subprocessing*) de dados e um maior detalhamento nas obrigações que devem ser assumidas uma vez finalizada a prestação dos serviços de tratamento dos dados pessoais.

Em suma, são todas proteções contratuais que visam garantir que a DNPDP possa exercer controle sobre a transferência de dados pessoais em caso de análise do contrato.

Finalmente, em 2023, por meio da Resolução nº 198/2023, a AAIP aprovou as novas cláusulas contratuais para a transferência internacional de dados que complementam, mas não substituem, as cláusulas-padrão contratuais que foram acolhidas pela Disposição 60/2016 da Direção Nacional de Proteção de Dados Pessoais. Essas novas cláusulas baseiam-se no modelo da Rede Ibero-Americana de Proteção de Dados (RIPD).

A adoção dessas SCCs representa um passo em direção à harmonização de normas e fluxos de dados entre a Argentina e outras jurisdições latino-americanas e da União Europeia.

4.6 Como se determina quando um país é adequado?

Existem vários modelos no Direito Comparado. Alguns países listam as jurisdições que consideram adequadas para fins de transferência de dados pessoais (regime conhecido como *white list* ou lista branca). Outros podem optar por listar países que não são considerados adequados, uma espécie de "lista negra". Finalmente, outros países podem optar por não listar um ou outro país adequado, mas sim aderir às aprovações feitas por outra jurisdição.

A Lei nº 25.326 não explicou em detalhes como se determina que um país ou organismo internacional é adequado para fins do artigo 12. Todavia, o decreto regulamentar estabeleceu certas diretrizes que permitem concluir quando um país é adequado.

O decreto regulamentar autorizou a DNPDP a "avaliar, de ofício ou a pedido da parte interessada, o nível de proteção proporcionado pelas normas de um Estado ou organismo internacional".

Se a DNPDP chegar à conclusão de que um Estado ou organismo não protege adequadamente os dados pessoais, a DNPDP deve submeter ao Poder Executivo Nacional (PEN) um projeto de decreto para emitir tal declaração. A norma exige um decreto apenas no caso de uma declaração de falta de adequação, não para o reconhecimento expresso ou positivo de um país como adequado. Isso dá validade à Disposição 60/2016. Na prática, esse "não reconhecimento" expresso nunca ocorreu. Ou seja, a legislação argentina permite criar uma "lista negra" de países não adequados, mas o país nunca exerceu essa faculdade. É compreensível que isso não tenha ocorrido por ser uma questão que certamente geraria atritos diplomáticos com o país ao qual a adequação é negada.

O Decreto Regulamentar nº 1.558/2001 também estabelece que

> o caráter adequado do nível de proteção que um país ou organismo internacional oferece será avaliado considerando todas as circunstâncias que envolvem uma transferência ou uma categoria de transferências de dados; em particular, levar-se-á em consideração a natureza dos dados, a finalidade e a duração do tratamento ou dos tratamentos previstos, o local de destino final, as normas de direito, gerais ou setoriais, vigentes no país em questão, bem como as normas profissionais, códigos de conduta e medidas de segurança em vigor nesses locais, ou que se apliquem a organismos internacionais ou supranacionais.

Finalmente, o decreto regulamentar dispõe que

> Entende-se que um Estado ou organismo internacional proporciona um nível adequado de proteção quando essa proteção deriva diretamente do ordenamento jurídico vigente, ou de sistemas de autorregulação, ou da proteção estabelecida pelas cláusulas contratuais que prevejam a proteção de dados pessoais.

A Disposição DNPDP 60 foi mais direta e, em seu artigo 3º, enuncia os países adequados. Não é necessário, então, fazer uma análise do país de destino da transferência, a menos que o país não esteja mencionado na lista do artigo 3º da Disposição DNPDP 60/2016. Nesse caso, a DNPDP deverá fazer uma análise interna para incluí-lo na lista, como ocorreu

com o Reino Unido após o Brexit, o que motivou sua posterior incorporação na lista do artigo 3º da Disposição nº 60.

4.7 Como saber se um país que não está na lista é adequado e que método deve ser usado para determiná-lo?

Para começar, se o país não estiver listado no artigo 3º da Disposição nº 60, nem tiver sido objeto de um reconhecimento expresso pela DNPDP, em princípio, ele não é considerado adequado. Por isso, é importante que a DNPDP amplie sua lista para incluir alguns países latino-americanos que são adequados e desenvolva um método para explicar como essa conclusão é alcançada.

Nesse sentido, entendemos que o mais conveniente para a Argentina seria adotar o método elaborado pela União Europeia para analisar a adequação de países estrangeiros, por meio de vários documentos de trabalho emitidos pelo WP29 (agora EDPB). Nesse contexto, o documento de trabalho da União Europeia concluiu que qualquer análise significativa de proteção adequada deve compreender dois elementos básicos: *i)* o conteúdo das normas aplicáveis; e *ii)* os meios para garantir sua aplicação eficaz.

Tomando a Diretiva 95/46/CE como ponto de partida, e considerando as disposições de outros textos internacionais sobre proteção de dados, o documento indica que deve ser possível alcançar um "núcleo" de princípios de "conteúdo" de proteção de dados e de requisitos "de procedimento e aplicação", cujo cumprimento possa ser considerado um requisito mínimo para julgar a proteção como adequada. Esse documento foi atualizado pelo EDPB após o RGPD.

O documento enuncia os seguintes princípios básicos (princípios de conteúdo): *i)* princípio de limitação de finalidade: os dados devem ser tratados com uma finalidade específica e posteriormente utilizados ou transferidos somente se não for incompatível com a finalidade da transferência; *ii)* princípio de proporcionalidade e qualidade dos dados: os dados devem ser exatos e, quando necessário, atualizados. Os dados devem ser adequados, pertinentes e não excessivos em relação à finalidade para o qual são transferidos ou tratados posteriormente; *iii)* princípio de transparência: os inte-

ressados devem ser informados sobre a finalidade do tratamento e a identidade do controlador do tratamento no país de destino, além de qualquer outro elemento necessário para garantir um tratamento justo; *iv)* princípio de segurança: o controlador do tratamento deve adotar medidas técnicas e organizacionais adequadas aos riscos que o tratamento apresenta. Qualquer pessoa que atue sob a autoridade do controlador pelo tratamento, incluindo o operador, não deve tratar os dados, exceto sob instrução do controlador; *v) direitos de acesso, retificação e oposição*: o interessado deve ter o direito de obter uma cópia de todos os seus dados e o direito de retificar os dados que sejam imprecisos. Em determinadas situações, o interessado também deve poder se opor ao tratamento dos dados que lhe dizem respeito; *vi)* restrições em relação a transferências subsequentes para outros países: as transferências subsequentes de dados pessoais do país de destino para outro país só devem ser permitidas se este último país garantir um nível de proteção adequado; *vii)* dados sensíveis: quando se tratar de categorias de dados "sensíveis", devem ser estabelecidas proteções adicionais, como a exigência de que o interessado dê seu consentimento explícito para o tratamento; *viii)* marketing direto: se a finalidade da transferência de dados for marketing direto, o interessado deve ter a possibilidade de recusar a qualquer momento que seus dados sejam utilizados para esse fim; e *ix)* decisão individual automatizada: quando a finalidade da transferência for a adoção de uma decisão automatizada nos termos do artigo 15 da diretiva, o interessado deve ter o direito de conhecer a lógica aplicada a essa decisão, e devem ser adotadas outras medidas para proteger o interesse legítimo da pessoa.

Em relação aos "mecanismos de procedimento e aplicação", o documento do WP29 explica que na Europa existe um amplo consenso de que um sistema de "supervisão externa" na forma de uma autoridade independente é uma característica necessária de um sistema de cumprimento da proteção de dados. No entanto, em outras partes do mundo, essas características nem sempre são encontradas.

Com o objetivo de estabelecer as bases para avaliar a adequação da proteção oferecida, é necessário distinguir os objetivos de um sistema normativo de proteção de dados e, com base nisso, julgar a variedade de diferentes mecanismos de procedimentos judiciais e não judiciais utilizados nos países de destino. Os objetivos de um sistema de proteção de dados são basicamente três: *i)* oferecer um nível satisfatório de cumprimento das

normas. Um bom sistema se caracteriza, em geral, pelo fato de que os controladores do tratamento conhecem bem suas obrigações e os interessados conhecem bem seus direitos e os meios para exercê-los. A existência de sanções efetivas e dissuasivas é importante para garantir a observância das normas, assim como são, naturalmente, os sistemas de verificação direta pelas autoridades, auditores ou serviços da administração especificamente encarregados da proteção de dados; *ii)* oferecer apoio e assistência aos interessados no exercício de seus direitos. O interessado deve ter a possibilidade de fazer valer seus direitos com rapidez e eficácia, e sem custos excessivos. Para isso, é necessário que haja algum tipo de mecanismo institucional que permita investigar as denúncias de forma independente; e *iii)* oferecer vias adequadas de recurso aos que forem prejudicados no caso de não observância das normas. Este é um elemento-chave que deve incluir um sistema que ofereça a possibilidade de obter uma resolução judicial ou arbitral e, se necessário, indenizações e sanções.

A Decisão da Comissão Europeia de 30 de junho 2003, de acordo com a Diretiva 95/46/CE do Parlamento Europeu e do Conselho sobre a adequação da proteção dos dados pessoais na Argentina, analisou o sistema legal de proteção de dados pessoais vigente na Argentina, com base nas diretrizes acima mencionadas, concluindo que este era adequado ao regime europeu, mas com algumas ressalvas. De fato, a decisão chamou a atenção para vários aspectos da lei argentina, que, a nosso ver, requerem uma reforma legislativa futura.

Com base nesses parâmetros, e após uma análise extensa, a Comissão da União Europeia, com a intervenção do *Working Party*, declarou que certos países latino-americanos, como é o caso da Argentina e do Uruguai, possuem proteção adequada. A Argentina seguiu este critério ao reconhecer os mesmos países mencionados na Disposição 60/2016.

5 Brasil

5.1 As transferências internacionais de dados no sistema brasileiro: a Lei Geral de Proteção de Dados Pessoais (LGPD) e a necessidade da regulação pela Autoridade Nacional de Proteção de Dados (ANPD)

A Lei nº 13.709/2018, conhecida como a Lei Geral de Proteção de Dados Pessoais (LGPD), estabelece regras para o tratamento de dados pessoais no Brasil e inclui normas específicas sobre transferências de dados pessoais. Entre os principais deveres estabelecidos pela legislação, destaca-se a necessidade de cumprir normas e procedimentos específicos para realizar transferências internacionais de dados pessoais.

Os mecanismos de transferência internacional de dados tornaram-se essenciais para o desenvolvimento da economia digital e, também, para garantir a eficácia dos direitos à proteção de dados pessoais. Esses mecanismos promovem a interoperabilidade legislativa[33] entre os diferentes sistemas normativos, a sustentabilidade dos fluxos de dados, que devem ser permitidos somente na medida em que não prejudiquem os direitos dos usuários.

Nesse contexto, é importante destacar que a LGPD consagra um mecanismo de aplicação extraterritorial de proteção de dados, independentemente da localização da sede da entidade ou da localização dos dados tratados, desde que os dados tratados se refiram a pessoas físicas localizadas no Brasil ou quando os dados pessoais tratados foram coletados no Brasil.

Os dados coletados no Brasil são considerados pertencentes ao titular que se encontrava no Brasil no momento da coleta. A LGPD também se aplica, independentemente da localização do território ou entidade, ou da localização onde os dados são tratados, se o objetivo da atividade de tratamento de uma entidade for oferecer ou fornecer bens ou serviços a pessoas físicas localizadas no Brasil.

33 BELLI, Luca; DONEDA, Danilo. Data Protection in the BRICS Countries: Legal Interoperability through Innovative Practices and Convergence. *International Data Privacy Law*, v. 13, n. 1, p.1-24, fev. 2023. Disponível em: https://doi.org/10.1093/idpl/ipac019.

Para compreender o funcionamento da disciplina brasileira de proteção de dados, é, portanto, necessário fornecer uma breve explicação terminológica preliminar, que será detalhada na seção seguinte.

5.2 Os conceitos de dados pessoais, a transferência internacional e os agentes de tratamento

Vale destacar que o artigo 5º, inciso X da LGPD inclui explicitamente a transferência como exemplo de atividade de tratamento, que envolve "toda operação realizada com dados pessoais". A transferência internacional é definida no artigo 5º, XV, como "a transferência de dados pessoais para um país estrangeiro ou para uma organização internacional da qual o país seja membro."

É importante entender que o conceito de transferência não se limita apenas ao envio de dados pessoais de um país para outro: o armazenamento de dados pessoais fora do país e o acesso remoto a dados pessoais do exterior também são considerados como uma transferência internacional para fins da legislação.

Além disso, a LGPD se inspirou na conceituação europeia de dado pessoal e define no artigo 5º, I como "informação relacionada a uma pessoa natural identificada ou identificável." No entanto, ao contrário do marco regulatório europeu, a LGPD não define o que é um "dado identificável", podendo, portanto, incluir um espectro extremamente amplo de dados cuja transferência deve estar sujeita ao regime estabelecido pela LGPD.

Destaca-se também que o marco regulatório brasileiro não se aplica a dados anonimizados, definidos como "dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento." No entanto, aplica-se igualmente a dados pessoais sensíveis, definidos como "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural"[34].

34 Ver LGPD artigo 5º, II e 5º, III.

Finalmente, a LGPD se aplica aos controladores de dados e aos operadores de dados, conhecidos conjuntamente como "agentes de tratamento",[35] que podem ser empresas, setores públicos, instituições, bem como organizações sem fins lucrativos. O artigo 5º, VI da LGPD define o controlador como a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões relativas ao tratamento de dados pessoais", ou seja, a entidade responsável por definir como os dados pessoais serão tratados, com quais finalidades e para quem. O artigo 5º, VII da LGPD define o operador como uma "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador", ou seja, a entidade que implementa as decisões tomadas pelo controlador.

5.3 As condições da transferência internacional de dados pessoais

A LGPD permite a transferência internacional de dados pessoais para países ou organizações internacionais que ofereçam um nível adequado de proteção de dados pessoais, ou quando o controlador garantir o cumprimento do regime de proteção de dados estabelecido em capítulo específico da LGPD.

O capítulo V da LGPD, denominado especificamente "Da Transferência Internacional de Dados", estabelece em seu artigo 33 as situações legais que autorizam a transferência internacional de dados pessoais e detalha os pilares da avaliação de adequação em seu artigo 34. O artigo 35 estabelece que a Autoridade Nacional de Proteção de Dados (ANPD) definirá o conteúdo das cláusulas-padrão contratuais, assim como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificações e códigos de conduta, descritos no inciso II do artigo 33. Até o momento da finalização deste trabalho, a ANPD ainda não havia concluído o processo de consulta pública. O resultado dessa consulta é importante para a definição desses elementos por meio do Regulamento de Transferências Internacionais de Dados Pessoais e das Cláusulas-Padrão Contratuais.[36] Além disso, o §1º do

35 Ver LGPD artigo 5º, IX.

36 Ver a consulta sobre o Regulamento de Transferências Internacionais de Dados Pessoais e do modelo de Cláusulas-Padrão Contratuais, disponível na *Plataforma Participa + Brasil*. 2023. Disponível em: https://bit.ly/3saZmag.

artigo 35 estabelece que, para a verificação prevista no artigo 35, devem ser considerados os requisitos, condições e garantias mínimas para o cumprimento dos direitos, garantias e princípios da LGPD ao transferir dados pessoais para outra jurisdição.

Particularmente, o artigo 33 é uma norma de maior relevância em relação às condições que devem ser cumpridas para regular a transferência internacional de dados. A norma estabelece que tal atividade está permitida nos seguintes casos:

> I. para países ou organizações internacionais que forneçam um nível adequado de proteção de dados pessoais conforme previsto nesta lei;
>
> II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
>
> a) cláusulas contratuais específicas para determinada transferência;
>
> b) cláusulas-padrão contratuais;
>
> c) normas corporativas globais;
>
> d) selos, certificados e códigos de conduta regularmente emitidos;
>
> III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
>
> IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> V - quando a autoridade nacional autorizar a transferência;
>
> VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
>
> VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
>
> VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; [...]

As opções estabelecidas no artigo 33 serão exploradas brevemente nas seções seguintes, enfatizando as principais vantagens e os principais limites de cada uma das condições previstas na LGPD.

5.4 Avaliação de adequação

A avaliação de adequação do nível de proteção de dados pessoais de países terceiros será realizada pela ANPD, que desempenha um papel central no âmbito da LGPD, sendo o "órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento desta lei." Os critérios que a ANPD deve seguir para realizar essa avaliação são definidos pelo artigo 34 da LGPD, segundo o qual a autoridade levará em consideração:

> I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;
>
> II - a natureza dos dados;
>
> III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;
>
> IV - a adoção de medidas de segurança previstas em regulamento;
>
> V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais;
>
> VI - outras circunstâncias específicas relativas à transferência.

Em agosto de 2024, a autoridade brasileira adotou a Resolução CD/ANPD nº 19, que aprova o Regulamento sobre Transferência Internacional de Dados Pessoais,[37] esclarecendo o mecanismo de avaliação do nível de proteção de dados de países estrangeiros ou organismos internacionais, bem como a definição do conteúdo das cláusulas-padrão em contratos, que também é de sua responsabilidade. Antes de apresentar o conteúdo da Resolução nº 19 de 2024, analisaremos brevemente o processo participativo que levou à sua elaboração.[38]

5.5. A tomada de subsídios e a consulta pública sobre transferência internacional de dados

Entre 2022 e 2023, a ANPD organizou processos participativos para construir sua abordagem regulatória em matéria de transferência de dados: primeiro, uma tomada de subsídios para receber sugestões e, depois, uma

37 Ver o Anexo A deste capítulo.

38 Ver consulta da ANPD disponível em: https://bit.ly/3D3z5MK.

consulta pública sobre sua proposta de Regulamento sobre Transferências Internacionais de Dados Pessoais e Cláusulas-Padrão Contratuais.[39]

O item 9 da agenda reguladora bienal 2021-2022 da ANPD, aprovada pela Portaria nº 11, de 27 de janeiro de 2021, refere-se à regulamentação da transferência internacional de dados pessoais, incluindo a avaliação do nível de proteção de dados de países estrangeiros ou organismos internacionais e a definição do conteúdo das cláusulas-padrão em contratos, que serão analisadas na próxima seção.

De acordo com o artigo 14 da Portaria ANPD nº 16/2021, que aprova o processo de regulamentação no âmbito da autoridade, a tomada de subsídios, bem como a coleta de dados e informações que a equipe da ANPD considerar relevantes, são considerados mecanismos de participação essenciais para a Análise de Impacto Regulatório (AIR).

A tomada de subsídios, no entanto, não deve ser confundida com uma simples consulta pública orientada para o debate de uma proposta de regulamentação. Pelo contrário, deve ser considerada uma fase preliminar, cuja função é prévia à elaboração de uma proposta de regulamentação para seu posterior debate. Portanto, ao ser realizada durante o processo de elaboração da proposta normativa, a tomada de subsídios é um instrumento adicional de democracia participativa que permite identificar e melhorar os aspectos significativos relacionados ao tema em questão, delimitando os problemas a serem abordados e as possíveis alternativas regulatórias.

Os resultados da tomada de subsídios, realizada entre maio e junho de 2022, foram consolidados no Relatório de Análise de Impacto Regulatório[40] e publicados em agosto de 2023, no âmbito da consulta pública sobre a proposta de regulamento.

O Relatório apresenta as alternativas regulatórias e seus impactos, com o objetivo de estabelecer mecanismos e procedimentos que permitam a transferência de dados, garantindo ao mesmo tempo o cumprimento e respeito aos princípios, diretrizes e fundamentos dispostos na LGPD. Particularmente, o documento detalha os resultados da tomada de subsídios

39 Ver nota 18.

40 Ver ANPD. Relatório de Análise de Impacto Regulatório: Construção do Modelo Regulatório para Transferência Internacional de Dados Pessoais. *ANPD*. 2023. Disponível em: https://bit.ly/3QqIbcP.

e enfatiza os caminhos regulatórios que deverão ser seguidos, com vistas a reduzir as externalidades negativas decorrentes da intervenção regulatória.

Nesse sentido, foram observados cinco principais temas a serem regulados: a definição de transferência internacional de dados pessoais; a definição de requisitos mínimos, condições e garantias para a transferência; o conteúdo das cláusulas-padrão contratuais, de acordo com o artigo 35, caput e §1; o processo de verificação de cláusulas contratuais específicas e das normas corporativas globais, de acordo com o artigo 33, II, a e c, e artigo 35, caput, e §§1º, 2º e 5º; e, finalmente, a definição da forma e prazos para comunicar mudanças nas garantias apresentadas.

Vale a pena destacar que o relatório revela uma certa preferência do regulador pelas cláusulas-padrão contratuais, destacando que "embora o art. 33 da Lei estabeleça diversas hipóteses que autorizam a transferência internacional de dados pessoais, observa-se que as Cláusulas-Padrão Contratuais têm sido uma das modalidades de transferência internacional de dados mais utilizadas, funcionando como ferramenta de convergência entre diferentes sistemas jurídicos."[41]

A definição de requisitos, condições e garantias mínimas para a transferência internacional de dados, por sua vez, deverá ajustar-se aos princípios gerais estabelecidos no artigo 6º da LGPD, como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização, sem a possibilidade legal de definir novos parâmetros ou limites.

O regulamento proposto na consulta de 2023 contém nove capítulos dedicados a *i)* disposições gerais; *ii)* definições; *iii)* transferência internacional de dados; *iv)* decisão de adequação; *v)* cláusulas-padrão contratuais; *vi)* cláusulas contratuais específicas; *vii)* normas corporativas globais; *viii)* processo de aprovação de cláusulas contratuais específicas e normas corporativas globais; e *ix)* disposições finais.

O terceiro capítulo, sobre a transferência internacional de dados, está estruturado em quatro seções dedicadas a: *i)* requisitos gerais; *ii)* caracterização da transferência internacional de dados; *iii)* aplicação da legislação nacional de proteção de dados pessoais; e *iv)* hipótese legal e modalidade de transferência. O objetivo deste capítulo é destacar que a transferência

41 Ibid. Parágrafo 15.

internacional de dados só poderá ser realizada para atender finalidades legítimas, específicas, explícitas e informadas ao titular, sem possibilidade de tratamento posterior de forma incompatível com tais finalidades.

O quinto capítulo, sobre cláusulas-padrão contratuais, está estruturado em duas seções: *i)* disposições gerais; *ii)* cláusulas-padrão contratuais equivalentes. Esta segunda seção é particularmente interessante porque destaca que a ANPD poderá reconhecer a equivalência das cláusulas-padrão contratuais de outros países ou organismos internacionais com as cláusulas estabelecidas no regulamento.

Apesar de ainda não ser definitiva, a estrutura do regulamento proposto nos permite entender como a ANPD está construindo sua abordagem. As seções seguintes elucidam brevemente as ferramentas alternativas à decisão de adequação, definidas na LGPD para permitir a transferência internacional de dados.

5.6 Cláusulas contratuais específicas e cláusulas-padrão contratuais

Como destacado no artigo 33, o controlador pode realizar a transferência internacional de dados pessoais por meio de cláusulas contratuais específicas, desde que essas cláusulas sejam devidamente verificadas e aprovadas pela autoridade. A LGPD não define o processo de avaliação das cláusulas contratuais específicas pela ANPD, e sua limitação está definida no artigo 35, que afirma que "na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário", e para realizar a verificação das cláusulas contratuais "deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei."

Além das cláusulas específicas, o artigo 33 da LGPD permite o uso de cláusulas-padrão contratuais formuladas pela ANPD. Essa ferramenta definirá, por meio de cláusulas-padrão, as responsabilidades das partes envolvidas na transferência e os direitos dos titulares dos dados que serão transferidos. Dessa forma, a adoção de cláusulas-padrão contratuais elaboradas pela

ANPD, uma vez aprovadas, se tornará uma ferramenta valiosa de conformidade normativa, demonstrando a integração dos requisitos e das responsabilidades estabelecidas nos contratos que regulam a transferência de dados pessoais, sem que a ANPD realize atividades posteriores de avaliação.

Infelizmente, a LGPD não define o conteúdo das cláusulas-padrão contratuais, sendo, portanto, necessária a atividade regulatória da ANDP, que foi iniciada com a tomada de subsídios mencionada anteriormente e concluída com a consulta pública que levou à adoção do Regulamento sobre Transferência Internacional de Dados Pessoais.[42]

Portanto, é importante destacar que às cláusulas-padrão contratuais representam um instrumento considerado particularmente promissor pela autoridade. Nesse contexto, nos parece que a recente adoção de um Guia de Implementação de Cláusulas-Padrão Contratuais para a Transferência Internacional de Dados Pessoais pela Rede Ibero-Americana de Proteção de Dados, da qual a ANPD é membro, representou um avanço que, certamente, influenciou o pensamento do regulador brasileiro.[43]

5.7 Normas corporativas globais

As normas corporativas globais (NCG) foram introduzidas na LGPD a partir das *Binding Corporate Rules* (BCR) típicas do sistema europeu, permitindo a transferência internacional de dados pessoais entre empresas do mesmo grupo econômico e, portanto, sujeitas à mesma política interna de proteção de dados pessoais. Destaca-se que, normalmente, as NCG de um determinado grupo econômico não se limitam à definição das condições das transferências internacionais. Elas são o documento que estabelece os procedimentos, as políticas e as medidas organizacionais e técnicas adotadas por todo o grupo para garantir a proteção de dados pessoais.

O artigo 33 da LGPD não fornece elementos para compreender como a conformidade das NCG será avaliada. No entanto, o artigo 35 estabelece a

42 ANPD. *Nota Técnica nº 20/2022/CGN/ANPD*, Assunto: Proposta de realização de Tomada de Subsídios para regulamentação de transferência internacional de dados pessoais, nos termos dos artigos 33 e 35 da LGPD da Lei nº 13.709, de 14 de agosto de 2018.

43 RIPD (Rede Ibero-Americana de Proteção de Dados). *Guía de Implementación de Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales*, 2022. Disponível em: https://bit.ly/3pDeH1P.

necessidade de verificação do conteúdo das normas pela autoridade, especificando que na "análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.

Por fim, o artigo 36 da LGPD acrescenta que as "alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional."

5.8 Selos, certificados e códigos de conduta

As partes envolvidas na transferência internacional de dados pessoais também podem utilizar selos, certificados ou códigos de conduta reconhecidos pela ANPD para realizar a transferência de forma compatível com a LGPD. O artigo 35 §1º estabelece que, para que a ANPD reconheça selos, certificados e códigos de conduta, eles devem cumprir os requisitos, as condições e as garantias mínimas para o cumprimento dos direitos, garantias e princípios da LGPD.

Além disso, o artigo 35 §3º acrescenta que a"autoridade nacional poderá designar organismos de certificação para a realização do previsto no *caput* deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento". No entanto, destacamos que esses elementos ainda não foram definidos pela ANPD.

5.9 Cooperação jurídica internacional

O artigo 33 também permite a transferência internacional de dados quando "a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional." Em relação a essa hipótese, é importante destacar que estão incluídas explicitamente as atividades de inteligência, investigação e persecução como circunstâncias em que a proteção do interesse público justifica a transferência de dados, apesar da falta de uma normativa em matéria de proteção de dados no âmbito dessas atividades no Brasil.

Assim como o Regulamento Geral de Proteção de Dados da União Europeia, a LGPD elimina sua aplicação para casos de tratamento de informações para a segurança pública e persecução penal. No entanto, ao contrário do sistema europeu, em que há uma legislação específica (a Diretiva nº 2016/680) que regulou a proteção de dados pessoais no âmbito das atividades de inteligência, investigação e persecução penal, no Brasil, a chamada "Lei Geral de Proteção de Dados Penal" nunca superou a fase de projeto de lei, não sendo adotada até o momento e deixando assim um importante vazio normativo.

5.10 Proteção da vida e da integridade física

A LGPD considera a proteção da vida ou da integridade física do indivíduo – seja dele mesmo ou de terceiros – como uma base legal para o tratamento de dados. Portanto, parece coerente que o artigo 35 §4º considere "a proteção da vida ou da incolumidade física" como uma justificativa válida para a transferência internacional de dados pessoais.

5.11 Autorização da ANPD

O inciso V do artigo 33 estabelece que a transferência internacional de dados pessoais pode ser realizada "quando a autoridade nacional autorizar a transferência". Essa norma pode se tornar uma verdadeira carta na manga para a ANPD, que tem uma notável discricionariedade – e potencial licença de criatividade – para regulamentar as transferências internacionais de dados na total ausência de procedimentos e critérios de avaliação estabelecidos pela LGPD.

5.12 Acordo de cooperação internacional

O inciso VI do artigo 33 estabelece que a transferência internacional de dados pessoais só é permitida "quando a transferência resultar em compromisso assumido em um acordo de cooperação internacional". Deve-se reconhecer que a redação dessa disposição cria uma notável confusão, já que, se interpretada literalmente, parece considerar a transferência como geradora do compromisso internacional.

Portanto, cabe destacar que essa norma deve ser considerada vítima de um erro de redação do legislador que, em vez de escrever "resultar em", deveria ter escrito "resultar de", sendo a transferência o resultado do compromisso internacional.

5.13 A Resolução CD/ANPD n. 19 que aprova o Regulamento sobre Transferência Internacional de Dados Pessoais

Em agosto 2024, a Autoridade Nacional de Proteção de Dados (ANPD) publicou a Resolução CD/ANPD nº 19, que aprova o Regulamento sobre Transferência Internacional de Dados Pessoais.[44] O regulamento estabelece normas fundamentais para a transferência internacional de dados pessoais, representando um marco significativo para os agentes de tratamento que operam em um cenário global e necessitam se adequar às disposições definidas no Capítulo V da LGPD.

O artigo 1º da Resolução aprova, na forma dos Anexos I e II incluídos na própria Resolução, o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais, nos termos do art. 33, incisos I e II, alíneas 'a', 'b' e 'c', art. 34, art. 35, caput e §§ 1º, 2º e 5º, e art. 36 da LGPD.

A normativa tem como fundamentos a proteção dos princípios definidos pela LGPD e os direitos dos titulares dos dados; a definição de incentivo a procedimentos simplificados e congruentes com as melhores práticas internacionais; a promoção do fluxo transfronteiriço de dados com confiabilidade, observando os direitos dos titulares; e, finalmente, a transparência e implementação de medidas de segurança apropriadas.

A Resolução CD/ANPD nº 19 reitera as hipóteses de aplicação da LGPD no que concerne às transferências internacionais, estabelecendo, ademais, que a lei brasileira será aplicável mesmo quando os dados sejam provenientes do exterior, desde que sejam objeto de tratamento em território nacional, ressalvados os casos excepcionais de: *i)* trânsito de dados sem comunicação ou uso por agentes de tratamento no Brasil; e *ii)* retorno dos dados tratados no Brasil a um país de origem que possua decisão de

44 Ver o Anexo A deste capítulo.

adequação emitida pela ANPD, com previsão expressa de não aplicabilidade da LGPD à operação. Com efeito, mostra-se importante ressaltar que a coleta internacional de dados não é considerada como transferência internacional para os fins da normativa.

A Resolução CD/ANPD nº 19 estabelece três mecanismos principais para a efetivação de transferências internacionais de dados. Em primeiro lugar, está a decisão de adequação, no âmbito da qual a ANPD realizará uma avaliação minuciosa do país ou organismo internacional para emitir a decisão de adequação. Esta análise considerará diversos fatores, incluindo, mas não se limitando, as normas e garantias judiciais existentes, a natureza dos dados envolvidos e os riscos e mecanismos de segurança implementados.

O regulamento enfatiza a importância de um órgão regulador independente para a decisão de adequação, embora não estabeleça tal critério como obrigatório. Além disso, a ANPD priorizará os países e organismos que assegurem reciprocidade. O processo de análise poderá ser iniciado pelo Conselho Diretor da ANPD, de ofício ou mediante solicitação da União (ou seja, o Governo Federal), Estados, Distrito Federal e Municípios.

Em segundo lugar, a Resolução CD/ANPD nº 19 admite o uso de cláusulas-padrão contratuais, cujo texto integral consta no anexo do regulamento. Tais cláusulas deverão ser adotadas sem alterações, cabendo ao agente apenas o preenchimento de acordo com as características específicas do tratamento de dados em questão. Cabe frisar que as cláusulas-padrão contratuais podem ser incorporadas a contratos genéricos ou específicos para a transferência.

Menciona-se, ainda, o fato de que o titular dos dados tem o direito de solicitar ao controlador a íntegra de tais cláusulas, devendo tal pedido ser atendido no prazo de 15 dias. Por sua vez, o controlador deverá manter informações em português sobre a transferência internacional, incluindo forma, duração, finalidade, país de destino e mecanismos de contato para exercício de direitos pelos titulares. Alternativamente, podem ser utilizadas cláusulas-padrão contratuais equivalentes, proferidas por outros organismos ou países, desde que previamente reconhecidas pela ANPD.

Em terceiro lugar, a Resolução CD/ANPD nº 19 admite o uso de normas corporativas globais, aplicáveis exclusivamente quando a transferência ocorrer entre agentes do mesmo grupo empresarial. Tais normas requerem aprovação prévia da ANPD e pressupõem a implementação de

um programa de privacidade e governança nos moldes estabelecidos pela LGPD. Os requisitos mínimos das Normas Corporativas Globais incluem a identificação: *i)* dos países envolvidos; *ii)* das finalidades do tratamento; *iii)* das bases legais utilizadas; e *iv)* dos tipos de dados tratados. A ANPD publicará em seu site a lista das Normas Corporativas Globais autorizadas, e o titular de dados poderá solicitar ao controlador a íntegra destas normas, observado o prazo de 15 dias para atendimento.

A Resolução autoriza, também, o uso de cláusulas contratuais específicas em situações excepcionais, quando as cláusulas-padrão contratuais não puderem ser utilizadas, circunstância esta que deverá ser comprovada pelo controlador. As cláusulas contratuais específicas devem seguir o texto das cláusulas-padrão contratuais tanto quanto possível, ser compatíveis com a LGPD e oferecer proteção similar às cláusulas-padrão contratuais. Tais cláusulas estão sujeitas à aprovação prévia da ANPD, mediante apresentação da documentação elencada no regulamento. O texto integral das cláusulas específicas aprovadas será disponibilizado no site da ANPD, ressalvadas as informações protegidas por segredo comercial e industrial.

A Resolução CD/ANPD nº 19 define ainda as obrigações dos agentes de tratamento no que diz respeito à:

- Limitação de dados: a transferência internacional deverá observar o princípio geralmente conhecido como "minimização dos dados", sendo executada limitando o tratamento ao mínimo necessário para a realização de finalidades específicas, legítimas e informadas, conforme ao artigo 6.III da LGPD. O regulamento enfatiza a impossibilidade de tratamento posterior com finalidade incompatível.
- Indicação da base legal: toda transferência internacional deve estar fundamentada em uma das bases legais previstas explicitamente nas hipóteses listadas pelo artigo 7º da LGPD.
- Transparência: os controladores devem manter informações atualizadas sobre as transferências internacionais em seus websites, incluindo detalhes sobre forma, duração, finalidade, país de destino e mecanismos de contato para exercício de direitos pelos titulares.

- Atendimento a solicitações dos titulares: os controladores devem estar preparados para atender, no prazo de 15 dias, às solicitações dos titulares referentes à íntegra das cláusulas-padrão contratuais, cláusulas específicas ou normas corporativas globais utilizadas nas transferências.

No que diz respeito à fiscalização, a ANPD está investida de poderes para exigir a apresentação dos contratos que utilizam as cláusulas-padrão contratuais, e solicitar alterações ou impor medidas adicionais, caso entenda que as cláusulas não são suficientes para garantir a proteção adequada dos dados transferidos. A Resolução CD/ANPD nº 19 concede um prazo de 12 meses para que os agentes que já utilizam cláusulas contratuais adequem seus instrumentos às cláusulas-padrão contratuais estabelecidas.

É importante ressaltar, por fim, que a Resolução CD/ANPD nº 19 representa um avanço significativo na regulamentação das transferências internacionais de dados pessoais no Brasil. Ao estabelecer critérios e mecanismos específicos, a normativa proporciona maior segurança jurídica aos agentes de tratamento, ao mesmo tempo em que visa garantir a proteção dos direitos dos titulares dos dados, facilitando o fluxo de informações e o comércio internacional.

Não obstante, é necessário frisar que a efetividade desta regulamentação dependerá diretamente da atuação incisiva da ANPD na fiscalização e na emissão tempestiva das decisões de adequação, bem como da capacidade dos agentes de tratamento em implementar as medidas necessárias para garantir a conformidade.

6 Colômbia

6.1 Nível adequado de proteção

A expressão "nível adequado de proteção" (NAPD) surgiu na Europa ao estabelecer regras para transferir dados pessoais para países terceiros. Ser considerado pela Europa como um país com tal nível de proteção não é simples nem rápido. Normalmente, exige que os países criem regulamentações apropriadas e façam mudanças institucionais. De fato, pode-se afirmar que

o artigo 25 da Diretiva (95/46/CE) foi o catalisador da necessidade de que muitos países regulamentassem o tratamento de dados pessoais e adotassem a abordagem europeia para poderem receber dados provenientes da Europa.

É importante notar que "nível adequado de proteção de dados pessoais" não significa estabelecer se um país tem um sistema de proteção idêntico ao de outro. Nesse sentido, o Tribunal de Justiça, por meio da sentença de 6 de outubro de 2015 no caso C362/14, de Maximillian Schrems contra o Comissário de Proteção de Dados[45] (Schrems), esclareceu que não é necessário que o país avaliado ou certificado tenha um nível de proteção idêntico, e que o importante é demonstrar que os meios utilizados pelo país em questão para proteger os dados pessoais sejam eficazes para garantir um nível adequado de proteção.[46]

Em linha com o anterior, na decisão de nível adequado dos Estados Unidos, de 10 de julho de 2023, a Comissão Europeia afirmou que: "o padrão de adequação não exige uma réplica ponto por ponto das normas da União. Mais especificamente, trata-se de determinar se, por meio da regulamentação sobre privacidade e sua implementação, supervisão e aplicação efetiva, o sistema estrangeiro, como um todo, fornece o nível necessário de proteção."[47] Como mencionado, garantir um nível adequado de proteção não exige que se garanta um nível idêntico ao da União Europeia, nem que as normas da União sejam reproduzidas literalmente. Isso foi afirmado pelo Tribunal de Justiça da União Europeia, pela Comissão Europeia e pelo European Data Protection Board (EDPB).

---

45 Tribunal de Justiça. *Caso C-362/14, Maximilian Schrems v. Data Protection Commissioner (Schrems), ECLI:EU:C:2015:650*, parágrafo 73.

46 Tribunal de Justiça. *Caso C-362/14, Maximilian Schrems v. Data Protection Commissioner (Schrems), ECLI:EU:C:2015:650*, parágrafo 74. Sobre nível adequado, também ler: Remolina Angarita, Nelson. 2024. "Is It Worthwhile for Latin American Countries to Obtain Adequate Level of Personal Data Protection from the European Approach or Is It Better to Promote the Use of Contractual Clauses to Export Such Information?". UNIO – EU Law Journal 10 (1):71-92. Disponível em: https://revistas.uminho.pt/index.php/unio/article/view/5856.

47 EUROPEAN UNION. *Commission Implementing Decision of 10.07.2023 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*. Brussels. 2023. Disponível em : https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf.

Conforme especificado no artigo 45, parágrafo 2, do Regulamento (UE) 2016/679,[48] a adoção de uma decisão de adequação deve basear-se em uma análise do ordenamento jurídico do país terceiro. A avaliação deve determinar se o país terceiro em questão garante um nível de proteção adequado ou equivalente, na essência, ao oferecido na União Europeia[49]. É relevante destacar que, segundo o Tribunal de Justiça da União Europeia, não se exige um nível de proteção idêntico.[50] Para esse tribunal, "é verdade que o termo ‹adequado› (…) significa que não se pode exigir que um terceiro país garanta um nível de proteção idêntico ao garantido no ordenamento jurídico da União."[51]

Sobre esse ponto, no caso "Schrems" o tribunal esclareceu que os meios existentes em outro país "devem ser eficazes na prática para garantir uma proteção substancialmente equivalente à garantida na União."[52] Em outras palavras, os mecanismos jurídicos de outros países (como a Colômbia) podem ser diferentes dos aplicados na União Europeia, desde que, na prática, sejam eficazes para garantir um nível adequado de proteção.[53] Segundo a Comissão Europeia, "o nível de adequação não exige que se reproduzam ao pé da letra as normas da União. Trata-se, mais precisamente, de determinar se o sistema estrangeiro, como um todo e pela essência dos direitos de privacidade e sua aplicação, força executiva e supervisão efetivas, oferece o nível de proteção exigido".[54] (Destaco).

---

48 UNIÓN EUROPEA. *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.* Strasbourg. 2016. (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE).

49 UNIÃO EUROPEIA. Cfr. Considerando 104 do Regulamento (UE) 2016/679. Bruxelas, 2016.

50 UNIÓN EUROPEA. *Cfr. Tribunal de Justicia (Gran Sala). Sentencia del 6 de octubre de 2015. Asunto C-362/14, Maximillian Schrem/Data Protection Commissioner.* Luxemburg, 2015. (en lo sucesivo, «Schrems»), ECLI:EU:C:2015:650, apartado 73. Disponível em: https://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=E.

51 Cfr. Schrems, apartado 73. Também ler o seguinte artigo: Remolina Angarita, Nelson. 2024. "Is It Worthwhile for Latin American Countries to Obtain Adequate Level of Personal Data Protection from the European Approach or Is It Better to Promote the Use of Contractual Clauses to Export Such Information?". UNIO – *EU Law Journal* 10 (1):71-92. Disponível em: https://revistas.uminho.pt/index.php/unio/article/view/5856.

52 Cfr. Schrems, apartado 74.

53 Cfr. Schrems, apartado 74.

54 UNIÃO EUROPEIA. Cfr. Comisión Europea. *DECISIÓN DE EJECUCIÓN (UE) 2019/419 DE LA COMISIÓN de 23 de enero de 2019 con arreglo al Reglamento (UE) 2016/679* del Parlamento

Tudo anterior foi reiterado pelo European Data Protection Board (EDPB) no documento intitulado "*Adequacy Referential*, WP 254 rev. 01".[55] Essencialmente, esse documento atualiza as diretrizes iniciais levando em conta a nova legislação[56] e a jurisprudência recente do Tribunal de Justiça da União Europeia (TJUE).[57] Em relação ao conceito e objetivo do nível adequado, destaca-se que: "embora o 'nível de proteção' no país terceiro deva ser 'substancialmente equivalente' ao garantido na União Europeia (UE), 'os meios utilizados por esse país terceiro para garantir esse nível de proteção podem ser diferentes dos aplicados na [UE]'. Portanto, o objetivo não é refletir ponto por ponto a legislação europeia, mas estabelecer os requisitos essenciais e básicos dessa legislação."[58]

O European Data Protection Board (EDPB) enfatiza que

> a adequação pode ser alcançada por meio de uma combinação de direitos para os titulares de dados e obrigações para aqueles que realizam o tratamento de dados, ou que exercem controle sobre tal tratamento, e a supervisão por parte de organismos independentes. No entanto, as normas de proteção de dados só são eficazes se forem aplicáveis e seguidas na prática. Portanto, deve-se levar em consideração não apenas o conteúdo das normas aplicáveis aos dados pessoais transferidos para um país terceiro ou organização internacional, mas também o sistema existente para garantir a efe-

Europeo y del Consejo, relativa a la adecuación de la protección de los datos personales por parte de Japón en virtud de la Ley sobre la protección de la información personal [notificada con el número C(2019) 304] (Texto pertinente a efectos del EEE). Considerando 3. O texto oficial está disponível em: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019D0419&from=SV.

55 EUROPEAN DATA PROTECTION BOARD. Adequacy Referential. WP 254 rev. 01. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

56 UNIÃO EUROPEIA. *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.* Unión Europea. 2016. (Regulamento geral de proteção de dados) (Texto pertinente a efeitos do EEE).

57 TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. *Assunto C-362/14, Maximillian Schrems contra Data Protection Commissioner, União Europeia, 6 de outubro de 2015*. Luxemburgo, 2014.

58 *European Data Protection Board, Adequacy Referential*, WP 254 rev. 01. p. 3. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

> tividade dessas normas. Mecanismos de aplicação eficientes são de vital importância para a eficácia das normas de proteção de dados.[59]

Tanto o conteúdo das normas aplicáveis, quanto os meios para garantir a aplicação efetiva delas, são cruciais, porque de nada servem as normas se não forem cumpridas. Nesse sentido, concordamos que "as normas sobre proteção de dados só contribuem para a proteção dos indivíduos se forem aplicadas na prática."[60]

A exportação e a importação de informações pessoais não podem se tornar um cenário de redução do nível de proteção conferido ao titular do dado no país de onde os dados pessoais são exportados. Para a Corte Constitucional da República da Colômbia, existem princípios que, apesar de não estarem numerados no artigo 4º da Lei Estatutária 1581 de 2012, são considerados incorporados nessa norma.[61] Um deles é o seguinte "princípio de exigência de padrões de proteção equivalentes para a transferência internacional de dados."

A Corte Constitucional reitera uma preocupação internacional dos Estados quando os dados de seus cidadãos circulam por suas fronteiras. Por isso, recorre ao critério europeu nessa matéria, no sentido de que os dados não devem ser enviados para países que não garantam um nível adequado de proteção. Para essa entidade, "como se deduz do artigo 26 do projeto de lei estatutária, existe uma proibição de transferência internacional para qualquer tipo de país que não forneça níveis adequados de proteção de dados".[62]

Estabelecer o nível adequado não é apenas uma questão formal de comparar os textos das normas locais com as do país para onde os dados serão exportados, mas também de avaliar os mecanismos de proteção real (administrativos, judiciais) disponíveis para o titular, para que seus dados

59 Ibid.

60 COMISSÃO EUROPEIA. **Cfr. Grupo de protección de las personas en lo que respecta al tratamiento de datos personales**. Bruxelas, 1997; UNIÓN EUROPEA. Primeras orientaciones sobre la transferencia de datos personales a países terceros: posibles formas de evaluar la adecuación. XV D/5020/97 -ES 2 WP4. Bruxelas. pp. 5. 1997; COMISSÃO EUROPEIA, Grupo de protección de las personas en lo que respecta al tratamiento de datos personales. União Europeia. 1998; UNIÃO EUROPEIA. Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE. DG XV D/5025/98 WP 12. Bruxelas. pp. 5. 1998.

61 Cfr. Corte Constitucional, Sentença C-748 de 2011. Numeral 2.6.6.2.

62 Cfr. Corte Constitucional, Sentença C-748 de 2011. Numeral 2.6.6.2.

sejam adequadamente protegidos em outro Estado, bem como de verificar a existência de autoridades de proteção de dados independentes, técnicas e eficientes. Em outras palavras, deve-se estabelecer o nível de proteção real que um país oferece na prática. No caso das autoridades de proteção, por exemplo, deve-se considerar o número de queixas recebidas dos cidadãos, bem como as ações iniciadas para responder a essas queixas, junto com as ordens ou sanções emitidas para proteger os direitos e punir os infratores da regulamentação sobre tratamento de dados.

Como é sabido, as regulamentações sobre transferência internacional de dados ou "fluxo transfronteiriço de dados" procuram garantir que o nível de proteção dos dados pessoais dos cidadãos de um país não diminua ou desapareça quando esses dados precisam ser exportados ou transferidos para outro(s) país(es). Por isso, no caso da regulamentação colombiana, por exemplo, é proibida "a transferência de dados pessoais de qualquer tipo para países que não forneçam níveis adequados de proteção de dados".[63]

A proibição de transferir dados para terceiros países que careçam de níveis adequados de proteção não é absoluta. Em certos casos excepcionais, isso é possível desde que sejam cumpridas as condições exigidas pela Lei nº 1581, pela jurisprudência da Corte Constitucional (C-748/2011) e pela eventual regulamentação sobre transferências internacionais. Em situações não previstas como exceções na lei citada, a SIC deve emitir uma declaração de conformidade em relação a essa transferência.[64]

6.2. Do reconhecimento da Colômbia como um país com nível adequado de proteção

A Superintendência de Indústria e Comércio (SIC) da República da Colômbia, como autoridade de proteção de dados pessoais, iniciou vários processos para obter reconhecimento de nível adequado de proteção de dados. Até

63 Cfr. República de Colômbia. Lei nº 1.581 de 2012. Artigo 26.

64 "En los casos no contemplados como excepción en el presente artículo, corresponderá a la Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el Superintendente queda facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación" (COLOMBIA. **par. 1º, artigo 26, Lei nº 1.581 de 2012.** Bogotá. 2012).

o momento, foi reconhecida pelo Centro Financeiro Internacional de Dubai como um país que oferece um nível adequado de proteção de dados pessoais.[65]

Essa foi a conclusão de 6 de outubro de 2022 do DIFC[66], Office of the Commissioner of Data Protection:

> It is for these reasons that the DIFC Office of the Commissioner of Data Protection ('the Commissioner') should grant adequacy recognition to Colombia. The current risk assessment regarding Colombia's laws and regulations, as well as the cultural and environmental approach to privacy and redress, align with the DIFC DP Law 2020 such that transfers to Colombia will receive the same or substantially equivalent protection when exported thereto"[67].

Além disso, desde 2019, a Colômbia iniciou conversas ou apresentou solicitações a outras organizações ou países com o propósito citado. Em todos os casos, foi fornecida, essencialmente, a mesma informação considerada pelo DIFC de Dubai.

TABELA 1 – Lista de solicitações realizadas pela Colômbia para obter decisão de adequação de proteção de dados pessoais

Organização ou país ao qual a Colômbia solicitou a decisão de adequação	Data de início do trâmite	Decisão
Comissão Europeia	Em 15 de outubro de 2019 se iniciaram conversas preliminares (Ofício 19-236409 do Superintendente Encarregado para a proteção de Dados da SIC).	Pendente
Reino Unido e Irlanda do Norte	Abril de 2021.	Pendente

65 Cfr. Superintendencia de Industria e Comércio (SIC). **Colombia es reconocida por su nivel adecuado de protección de datos por el Centro Financiero de Dubái.** Governo da Colômbia.18 de outubro de 2022. Disponível em: https://bit.ly/colombiareconoceadubai.

66 Dubai International Financial Centre Authority.

67 Cfr. Dubai International Financial Centre Authority ("DIFC" or "DIFCA"). *Commissioner of Data Protection. Assessment of Colombia's Data Protection Regime as Substantially Equivalent.* DIFCA. 2022. Disponível em: https://bit.ly/aereconoceimientocolombia.

Argentina	31 de agosto de 2021 (Ofício 21-348053 do Superintendente Encarregado para a proteção de Dados da SIC).	Pendente
Uruguai	31 de agosto de 2021 (Ofício 21-348062 do Superintendente Encarregado para a proteção de Dados da SIC).	Pendente

(Dados vigentes em 3 de junho de 2024).

6.3 Dos reconhecimentos de nível adequado de proteção de dados concedidos pela Colômbia a outros países

Para efeitos da circulação transfronteiriça de dados, a Superintendência de Indústria e Comércio (SIC), desde agosto de 2017, estabeleceu que os seguintes países possuem nível adequado de proteção de dados[68]: Alemanha; Austrália; Áustria; Bélgica; Bulgária; Chipre; Costa Rica; Croácia; Dinamarca; Eslováquia; Eslovênia; Estônia; Espanha; Estados Unidos da 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; Suécia; e os países que foram declarados com nível adequado de proteção pela Comissão Europeia (Suíça; Canadá; Argentina; Guernsey; Ilha de Man; Jersey; Ilhas Faroe; Andorra; Israel; Uruguai; Nova Zelândia e Japão).

Ao mesmo tempo, a SIC, mediante a Circular Externa 5, de 10 de agosto de 2017, ordenou o seguinte no primeiro parágrafo do numeral 3.2:

> Sem prejuízo de que as transferências de dados pessoais sejam realizadas para países que tenham um nível adequado de proteção, os controladores do tratamento, em virtude do princípio de responsabilidade demonstrada, devem ser capazes de demonstrar que implementaram medidas apropriadas e efetivas para garantir o adequado tratamento dos dados pessoais que transferem para ou-

68 Cfr. SIC Circulares externas, 5 e 8 de 2017 e 2 de 2018.

> tro país e para conceder segurança aos registros no momento de efetuar essa transferência.[69]

Como se observa, para transferir dados a outros países, não é suficiente que o país de destino esteja catalogado pela SIC como um país com nível adequado de proteção; é necessário também que o controlador do tratamento possa demonstrar que tomou medidas adequadas, úteis e práticas para alcançar estes dois objetivos:

> 1. Garantir o adequado tratamento dos dados pessoais que são transferidos para outro país.
>
> 2. Assegurar a segurança dos "registros no momento de efetuar essa transferência".

6.4. O que exige a autoridade colombiana de proteção de dados para estabelecer se um país tem nível adequado de proteção de dados?

A regulamentação colombiana é enfática ao indicar com absoluta clareza que os padrões estabelecidos para determinar se um país possui tal nível "em nenhum caso poderão ser inferiores"[70] aos da Lei nº 1.581 de 2012. Como se observa, no caso colombiano, não se pode enviar dados a um país que tenha um grau de proteção inferior ao previsto na referida norma.[71]

---

69 Cfr. o numeral 3.2 da Circular 5 de 2017 da SIC.

70 COLÔMBIA. Cfr. **Lei nº 1.581 de 2012, artigo 26.** Bogotá. 2012.

71 É o que diz o artigo 26 da Lei Estatutaria nº 1.581 de 2012:
Artículo 26. Prohibición. Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios.
Esta prohibición no regirá cuando se trate de:
a) Información respecto de la cual el titular haya otorgado su autorización expresa e inequívoca para la transferencia;
b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del titular por razones de salud o higiene pública;
c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable;

Para estabelecer que outro país cumpre com o nível adequado, devem-se levar em conta os padrões que a SIC estabelecer para esse propósito, os quais, segundo a parte final do primeiro parágrafo do artigo 26 da Lei nº 1.581 de 2012, "em nenhum caso poderão ser inferiores aos que a presente lei exige de seus destinatários."

A autoridade colombiana de proteção de dados, mediante a Circular 5, de 10 de agosto de 2017, da SIC estabeleceu o seguinte que foi incorporado no numeral 3.1. do capítulo V (Proteção de dados) da Circular Única dessa entidade:

> A análise para estabelecer se um país oferece um nível adequado de proteção de dados pessoais, para efeitos de realizar uma transferência internacional de dados, estará orientada a determinar se tal país garante a proteção dos mesmos, com base nos seguintes padrões:
>
> a) Existência de normas aplicáveis ao tratamento de dados pessoais.
>
> b) Consagração normativa de princípios aplicáveis ao tratamento de dados, entre outros: legalidade, finalidade, liberdade, veracidade ou qualidade, transparência, acesso e circulação restrita, segurança e confidencialidade.
>
> c) Consagração normativa de direitos dos Titulares.
>
> d) Consagração normativa de deveres dos Controladores e Operadores.

---

d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad;

e) Transferencias necesarias para la ejecución de un contrato entre el titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del titular;

f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

Par. 1.º - En los casos no contemplados como excepción en el presente artículo, corresponderá a la Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el superintendente queda facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

Par. 2.º - Las disposiciones contenidas en el presente artículo serán aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266 de 2008.

> e) Existência de meios e vias judiciais e administrativas para garantir a tutela efetiva dos direitos dos Titulares e exigir o cumprimento da lei.
>
> f) Existência de autoridade(s) pública(s) encarregada(s) da supervisão do tratamento de dados pessoais, do cumprimento da legislação aplicável e da proteção dos direitos dos titulares, que exerça(m) de maneira efetiva suas funções."[72]

6.5 Da flexibilidade para exportar dados da Colômbia para outros países

Embora a Lei Estatutária seja rigorosa nas regras de transferências internacionais, essas diretrizes foram modificadas por uma norma de hierarquia inferior, como a referida Circular 5, de 10 de agosto de 2017, da SIC. Essa circular ainda está em vigor e não foi declarada nula, razão pela qual tem plena aplicabilidade.

Nessa circular foram criados outros caminhos não previstos na Lei nº 1.581 de 2012 para exportar dados da Colômbia para outros países. Indica o seguinte, que foi incorporado no item 3.2 do capítulo V (Proteção de Dados) da Circular Única da SIC: Quando a transferência de dados pessoais for realizada para um país que não esteja entre os considerados com nível adequado pela SIC, o Controlador do tratamento deve:

> a) Verificar se a transferência está compreendida em uma das exceções estabelecidas no artigo 26 da Lei nº 1.581 de 2012; ou,
>
> b) "**Se esse país cumpre com os padrões estabelecidos pela SIC, casos em que poderá realizar a transferência**". (Destacamos). Como se observa, a SIC permite que os exportadores de dados estabeleçam se determinado país cumpre os padrões fixados por essa entidade, sem a necessidade de uma avaliação prévia pela SIC. Isso não está previsto na Lei nº 1.518 de 2012 e representa uma clara extrapolação dos poderes regulamentares dessa entidade, pois a circular amplia o conteúdo

72 COLÔMBIA**. Cfr. Numeral 3.1 do capítulo V (Proteção de dados) da Circular Única da SIC**. 2017: Disponível em: https://bit.ly/44vCX4T.

> e alcance de uma Lei Estatutária, estabelecendo uma nova regra que não foi criada pelo legislador.
>
> c) Se nenhuma das hipóteses anteriores for cumprida, "solicitar a respectiva declaração de conformidade perante esta Superintendência."
>
> Adicionalmente, em relação à declaração de conformidade, a SIC criou a seguinte regra não prevista na Lei Estatutária nº 1.581 de 2012:
>
> Parágrafo: Quando os Controladores do Tratamento, com o objetivo de cumprir o princípio de responsabilidade demonstrada, firmarem um contrato com o Controlador do Tratamento destinatário dos dados ou implementarem outro instrumento jurídico pelo qual se estabeleçam as condições que regerão a transferência internacional de dados pessoais e que garantirão o cumprimento dos princípios que regem o tratamento, assim como das obrigações que têm a seu cargo, se presumirá que a operação é viável e que conta com a Declaração de Conformidade.
>
> Consequentemente, os Controladores do Tratamento poderão realizar essa transferência, após comunicação enviada à *Delegatura para la Protección de Datos Personales* da Superintendência de Indústria e Comércio, na qual informem sobre a operação a ser realizada e declarem que assinaram o contrato de transferência ou outro instrumento jurídico que garanta a proteção dos dados pessoais objeto de transferência, o que poderá ser verificado a qualquer momento por esta Superintendência e, caso seja constatado algum descumprimento, poderá ser iniciada a investigação correspondente, impondo-se as sanções cabíveis e ordenando as medidas que forem necessárias.[73]

Apesar de sua utilidade, a assinatura de um contrato de transferência ou instrumento jurídico não está prevista na Lei nº 1.581 de 2012 como substituto da declaração de conformidade.

---

73 COLÔMBIA. **Cfr. Numeral 3.3 do capítulo V (Proteção de dados) da Circular Única da SIC**. Disponível em: https://bit.ly/3Df4tb.

7 México

7.1 Introdução

Os dados pessoais são definidos como qualquer informação relacionada a uma pessoa física identificada ou identificável, entendida como aquela cuja identidade pode ser determinada de forma direta ou indireta por meio de qualquer informação.

A proteção de nossos dados pessoais é um dos elementos que integram o conceito de privacidade. A esse respeito, alguns autores consideram necessário distinguir entre os termos *privacidade* e *intimidade*, visto que a visão norte-americana contempla a privacidade como o direito de estar isolado e não ser sujeito à publicidade ou escrutínio.[74]

No entanto, o ordenamento jurídico nacional em matéria de proteção de dados pessoais no México está estruturado com base em uma classificação que atende à natureza pública ou privada daqueles que realizam o tratamento de dados pessoais, ou seja, dos controladores.

O direito humano à proteção de dados pessoais está inscrito no artigo 16 da Constituição Política dos Estados Unidos Mexicanos (CPEUM), reconhecendo que todas as pessoas têm direito à proteção de seus dados pessoais, ao acesso, retificação e exclusão, bem como a manifestar sua oposição, nos termos estabelecidos por lei.

O acima exposto, em conformidade com o artigo 1º da Constituição, reconhece que todas as pessoas gozarão dos direitos humanos previstos nesta e nos tratados internacionais dos quais o Estado mexicano seja parte, estabelecendo a aplicação do princípio pro persona para a interpretação das normas relativas aos direitos humanos.

74 CIENFUEGOS SALGADO, David. El derecho a la intimidad y los actos procesales de imposible reparación. La tesis 1a/J17/2003, sobre admisión y desahogo de la prueba pericial en genética. *Revista Lex*, México, n. 101. pp. 47 e 203. 2003.

7.2 Antecedentes normativos no México

A partir da reforma constitucional publicada no Diário Oficial da Federação, em 1º de junho de 2009,[75] foi adicionado um parágrafo ao artigo 16 da Constituição Política dos Estados Unidos Mexicanos, no qual se dispôs que toda pessoa tem direito à proteção de seus dados pessoais, ao acesso, retificação e exclusão deles, bem como a manifestar sua oposição, nos termos fixados pela lei.

Com base nisso, em 5 de julho de 2010, foi publicada no Diário Oficial da Federação a Lei Federal de Proteção de Dados Pessoais em Posse dos Particulares[76] (LFPDPPP), que tem por objetivo a proteção dos dados pessoais em posse de pessoas físicas ou jurídicas de direito privado (particulares), a fim de regular seu tratamento legítimo, controlado e informado, com a finalidade de garantir a privacidade e o direito à autodeterminação informativa das pessoas.

Essa normativa tem como exceções as sociedades de informação creditícia nos casos previstos pela legislação que as regula, assim como as pessoas que realizam a obtenção e armazenamento de dados pessoais para uso exclusivamente pessoal e sem fins de divulgação ou utilização comercial.

Por outro lado, é necessário fazer referência ao decreto de reforma constitucional em matéria de transparência, publicado no Diário Oficial da Federação, em 7 de fevereiro de 2014[77], pelo qual foi estabelecido que a federação teria um organismo autônomo, especializado, imparcial, colegiado, com personalidade jurídica e patrimônio próprio, responsável por garantir o cumprimento do direito de acesso à informação pública e à proteção de dados pessoais em posse dos sujeitos obrigados, nos termos

75 Decreto que acrescenta um segundo parágrafo, com os parágrafos subsequentes em sua ordem: MÉXICO. *artículo 16 de la Constitución Política de los Estados Unidos Mexicanos*. Cidade do México. 2009. Disponível em: https://bit.ly/40pHXHg.

76 MÉXICO. *Decreto por el cual se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*. Cidade do México. 2010. Disponível em: https://bit.ly/3Mx0VWW.

77 MÉXICO. *Decreto por el cual se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia*. Cidade do México, 2014. Disponível em: https://bit.ly/3FHQFHz.

estabelecidos na lei, criando o atual Instituto Nacional de Transparência, Acesso à Informação e Proteção de Dados Pessoais (INAI).

Além disso, na mesma reforma constitucional foram adicionadas as frações XXIX-S e XXIX-T ao artigo 73 da Constituição Política dos Estados Unidos Mexicanos, para conferir atribuições ao Congresso da União para expedir as leis gerais regulamentadoras que desenvolvam os princípios e bases em matéria de transparência governamental, acesso à informação e proteção de dados pessoais em posse das autoridades, entidades, órgãos e organismos governamentais de todos os níveis de governo.

Finalmente, em 26 de janeiro de 2017, foi publicada no Diário Oficial da Federação a Lei Geral de Proteção de Dados Pessoais em Posse de Sujeitos Obrigados[78] (LGPDPPSO), que tem por objetivo estabelecer as bases, princípios e procedimentos para garantir o direito das pessoas à proteção de seus dados pessoais em posse de sujeitos obrigados, entendidos como qualquer autoridade, entidade, órgão e organismo dos Poderes Executivo, Legislativo e Judiciário, órgãos autônomos, partidos políticos, fideicomissos e fundos públicos, nos âmbitos federal, estadual e municipal.

7.3 Instrumentos internacionais relevantes dos quais o México faz parte

A Declaração Universal dos Direitos Humanos, em seu artigo 12, estabelece que "Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques."

A Declaração Americana dos Direitos e Deveres do Homem, no artigo 5, intitulado "Direito à proteção da honra, reputação pessoal e vida privada e familiar", afirma que "Toda pessoa tem o direito à proteção da lei contra ataques abusivos à sua honra, à sua reputação e vida privada e familiar."

O Pacto Internacional de Direitos Civis e Políticos, no artigo 17, estabelece que ninguém será sujeito a interferências arbitrárias ou ilegais em sua vida privada, sua família, seu domicílio ou sua correspondência, nem a ataques ile-

78 MÉXICO. *Decreto por el cual se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*. Cidade do México, 2017. Disponível em: https://bit.ly/3Mrl1ll.

gais à sua honra e reputação. Da mesma forma, é estabelecido que toda pessoa tem o direito à proteção da lei contra essas interferências ou ataques.

A Convenção Americana sobre Direitos Humanos, no artigo 11, sobre "Proteção da Honra e da Dignidade", estabelece três pontos: "Toda pessoa tem direito ao respeito à sua honra e ao reconhecimento de sua dignidade"; "Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação"; e "Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas".

No artigo 16 da Convenção sobre os Direitos da Criança, é determinado que crianças e adolescentes têm o direito ao respeito pela sua privacidade, sendo responsabilidade do Estado proteger esse direito. Nesse sentido, estabelece-se:

> 1. Nenhuma criança será sujeita a interferências arbitrárias ou ilegais em sua vida privada, sua família, seu domicílio ou sua correspondência, nem a ataques ilegais à sua honra e reputação.
>
> 2. A criança tem o direito à proteção da lei contra essas interferências ou ataques.

Além disso, na Convenção Internacional sobre a Proteção dos Direitos de Todos os Trabalhadores Migrantes e Membros de Suas Famílias, especificamente no artigo 14, estabelece-se que "Nenhum trabalhador migrante ou membro da sua família será sujeito a intromissões arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio, na sua correspondência ou outras comunicações, nem a ofensas ilegais à sua honra e reputação. Os trabalhadores migrantes e membros da sua família têm direito à proteção da lei contra tais intromissões ou ofensas." Da mesma forma, aceita-se o direito dos trabalhadores mencionados e de seus entes queridos a receber proteção legal no território onde se encontrem.

A Convenção sobre os Direitos das Pessoas com Deficiência inclui o artigo 22, "Respeito à privacidade", que reconhece o direito das pessoas com deficiência à privacidade de seu lar, correspondência, honra e reputação. Especificamente, o segundo parágrafo estabelece que os Estados devem proteger a privacidade das informações pessoais e relacionadas à saúde e reabilitação das pessoas com deficiência em igualdade de condições com as demais.

A Convenção 108 foi o primeiro instrumento juridicamente vinculante em escala internacional adotado no que diz respeito à proteção de dados. De acordo com o primeiro artigo dessa convenção, seu objetivo é garantir, dentro do território de cada parte, o respeito pelos direitos e liberdades fundamentais de toda pessoa física, independentemente de sua nacionalidade ou local de residência. Isso se refere especificamente ao direito à privacidade em relação ao tratamento automatizado dos dados pessoais dessa pessoa ("proteção de dados").

Em 28 de setembro de 2018, foi publicado no Diário Oficial da Federação o Decreto Promulgatório da Convenção para a Proteção das Pessoas em relação ao Tratamento Automatizado de Dados de Caráter Pessoal, que foi adotado em Estrasburgo, França, em 28 de janeiro de 1981.

Com base nos tratados internacionais e documentos mencionados, pode-se inferir que:

- O México assinou vários acordos internacionais que reconhecem a importância dos direitos à privacidade e à vida privada. Entre esses instrumentos estão a Declaração Universal dos Direitos Humanos, a Declaração Americana dos Direitos e Deveres do Homem, o Pacto Internacional de Direitos Civis e Políticos, a Convenção Americana de Direitos Humanos, a Convenção sobre os Direitos da Criança, a Convenção Internacional sobre a Proteção dos Direitos de Todos os Trabalhadores Migrantes e Membros de Suas Famílias, a Convenção sobre os Direitos das Pessoas com Deficiência e a Convenção 108;
- Um dos acordos internacionais mais relevantes em matéria de direitos humanos que o México assinou é a Convenção 108, que foi aprovada pela Câmara de Senadores, em 26 de abril de 2018, e cujo decreto foi publicado no DOF, em 12 de junho do mesmo ano. O Poder Executivo Federal assinou o instrumento de adesão a essa convenção em 19 de junho de 2018 e o depositou junto ao Secretário-Geral do Conselho da Europa em 28 de junho de 2019. A adesão a essa convenção é importante tanto para o Estado mexicano em termos políticos e econômicos quanto para as pessoas, pois esse instrumento regula um direito humano fundamental;

- Por outro lado, o Acordo Estados Unidos-México-Canadá (USMCA/T-MEC) estipula que os países participantes cooperarão e manterão um diálogo sobre a promoção e o desenvolvimento de mecanismos que melhorem a interoperabilidade global dos regimes de privacidade, incluindo os CBPR;
- A situação geográfica do México o coloca em uma forte relação comercial com os Estados Unidos da América e o Canadá, por isso espera-se melhorar a relação comercial digital e a interoperabilidade entre seus marcos de privacidade. Além disso, a implementação total dos CBPR poderia posicionar esses três países para trabalhar como parceiros estratégicos na promoção da adoção dos CBPR em nível regional;
- Os acordos jurídicos mencionados demonstram que o Estado Mexicano está comprometido com a proteção efetiva dos direitos à privacidade, à vida privada e à proteção de dados pessoais. É importante destacar que a Rede Ibero-Americana de Proteção de Dados (RIPD), atualmente presidida pelo INAI, elaborou os Padrões de Proteção de Dados Pessoais (PPDP), que são disposições modernas que estabelecem princípios e direitos para a proteção de dados pessoais. Esses princípios podem ser adotados e desenvolvidos pelos Estados ibero-americanos em suas próprias legislações nacionais, com o objetivo de garantir um tratamento adequado dos dados pessoais.

7.4 Transferências nacionais e internacionais de dados de caráter pessoal

As transferências internacionais de dados são de grande importância na atualidade devido à globalização e à natureza cada vez mais interconectada da nossa sociedade. Em um mundo cada vez mais digital, as empresas e organizações ao redor do mundo precisam transferir dados constantemente entre diferentes países e regiões para realizar suas atividades e operações diárias.

Os modelos de proteção para as transferências de dados pessoais podem variar bastante, dependendo da região em que são realizadas. No Mé-

xico, a Lei adota um modelo próprio, mas seu texto e regulamento também podem ser analisados à luz de dois dos principais enfoques em matéria de privacidade no mundo: o europeu e o norte-americano, sem esquecer que é essencial garantir os direitos pessoais, mas também não obstruir o desenvolvimento comercial e global.

No marco normativo mexicano, as transferências nacionais e internacionais de dados de caráter pessoal estão reguladas tanto na Lei Federal de Proteção de Dados Pessoais em Posse de Particulares quanto na Lei Geral de Proteção de Dados Pessoais em Posse de Sujeitos Obrigados.

Para o setor privado, a Lei Federal estabelece, em seu capítulo V, "Transferências nacionais e internacionais de dados de caráter pessoal", artigos 36 e 37, e em seu Regulamento, nos artigos 37, 38 e 39, os quais dispõem:

> **Artigo 36.** Quando o controlador pretender transferir os dados pessoais a terceiros nacionais ou estrangeiros, diferentes do operador, deverá comunicar a estes o aviso de privacidade e as finalidades às quais o titular sujeitou o tratamento. O tratamento dos dados será realizado conforme o acordado no aviso de privacidade, que conterá uma cláusula indicando se o titular aceita ou não a transferência de seus dados; da mesma forma, o terceiro receptor assumirá as mesmas obrigações que correspondem ao controlador que transferiu os dados.
>
> **Artigo 37.** As transferências nacionais ou internacionais de dados poderão ser realizadas sem o consentimento do titular quando ocorrerem em um dos seguintes casos:
>
> I. Quando a transferência estiver prevista em uma Lei ou Tratado em que o México seja parte;
>
> II. Quando a transferência for necessária para a prevenção ou diagnóstico médico, prestação de assistência sanitária, tratamento médico ou gestão de serviços de saúde;
>
> III. Quando a transferência for efetuada a sociedades controladoras, subsidiárias ou afiliadas sob o controle comum do controlador, ou a uma sociedade matriz ou qualquer sociedade do mesmo grupo do controlador que opere sob os mesmos processos e políticas internas;
>
> IV. Quando a transferência for necessária em virtude de um contrato celebrado ou a celebrar em interesse do titular, pelo controlador e um terceiro;

> V. Quando a transferência for necessária ou legalmente exigida para a salvaguarda de um interesse público, ou para a procuradoria ou administração da justiça;
>
> VI. Quando a transferência for necessária para o reconhecimento, exercício ou defesa de um direito em um processo judicial; e
>
> VII. Quando a transferência for necessária para a manutenção ou cumprimento de uma relação jurídica entre o controlador e o titular.

Para o setor público, de acordo com a Lei Geral, o Capítulo Único "Das Transferências e Remissões de Dados Pessoais", artigos 65 a 71, dispõe:

> **Artigo 65.** Toda transferência de dados pessoais, seja nacional ou internacional, está sujeita ao consentimento do titular, salvo as exceções previstas nos artigos 22, 66 e 70 desta Lei.
>
> **Artigo 66.** Toda transferência deve ser formalizada mediante a assinatura de cláusulas contratuais, convênios de colaboração ou qualquer outro instrumento jurídico, de acordo com a normativa aplicável ao controlador, que permita demonstrar o alcance do tratamento dos dados pessoais, bem como as obrigações e responsabilidades assumidas pelas partes.
>
> O disposto no parágrafo anterior não será aplicável nos seguintes casos:
>
> I. Quando a transferência for nacional e realizada entre controladores em virtude do cumprimento de uma disposição legal ou no exercício de atribuições expressamente conferidas a estes; ou
>
> II. Quando a transferência for internacional e prevista em uma lei ou tratado assinado e ratificado pelo México, ou realizada a pedido de uma autoridade estrangeira ou organismo internacional competente na qualidade de receptor, desde que as atribuições entre o controlador transferente e o receptor sejam homogêneas, ou que as finalidades que motivaram a transferência sejam análogas ou compatíveis com aquelas que deram origem ao tratamento do controlador que realiza a transferência.
>
> **Artigo 67.** Quando a transferência for nacional, o receptor dos dados pessoais deve tratar os dados pessoais comprometendo-se a garantir sua confidencialidade e a utilizá-los exclusivamente para os fins para os quais foram transferidos, respeitando o acordado no aviso de privacidade que lhe será comunicado pelo controlador transferente.
>
> **Artigo 68.** O controlador só poderá transferir ou remeter dados pessoais para fora do território nacional quando o terceiro receptor ou o operador se comprometer a proteger os dados pessoais conforme os princípios e deveres estabelecidos nesta Lei e nas disposições aplicáveis na matéria.

Artigo 69. Em toda transferência de dados pessoais, o controlador deve comunicar ao receptor dos dados pessoais o aviso de privacidade com base no qual os dados pessoais são tratados em relação ao titular.

Artigo 70. O controlador poderá realizar transferências de dados pessoais sem necessidade de obter o consentimento do titular, nos seguintes casos:

I. Quando a transferência estiver prevista nesta Lei ou em outras leis, convenções ou Tratados Internacionais assinados e ratificados pelo México;

II. Quando a transferência for realizada entre controladores, desde que os dados pessoais sejam utilizados para o exercício de faculdades próprias, compatíveis ou análogas com a finalidade que motivou o tratamento dos dados pessoais;

III. Quando a transferência for legalmente exigida para a investigação e perseguição de crimes, bem como para a procuradoria ou administração da justiça;

IV. Quando a transferência for necessária para o reconhecimento, exercício ou defesa de um direito perante autoridade competente, desde que haja requerimento desta última;

V. Quando a transferência for necessária para a prevenção ou diagnóstico médico, prestação de assistência sanitária, tratamento médico ou gestão de serviços de saúde, desde que esses fins sejam comprovados;

VI. Quando a transferência for necessária para a manutenção ou cumprimento de uma relação jurídica entre o controlador e o titular;

VII. Quando a transferência for necessária em virtude de um contrato celebrado ou a celebrar em interesse do titular, pelo controlador e um terceiro;

VIII. Quando se tratar de casos em que o controlador não esteja obrigado a obter o consentimento do titular para o tratamento e transmissão de seus dados pessoais, conforme disposto no artigo 22 da presente Lei; ou

IX. Quando a transferência for necessária por razões de segurança nacional.

A atualização de algumas das exceções previstas neste artigo não exime o controlador de cumprir as obrigações previstas no presente Capítulo que sejam aplicáveis.

Artigo 71. As remissões nacionais e internacionais de dados pessoais realizadas entre controlador e operador não necessitam ser informadas ao titular, nem obter seu consentimento.

7.5 Conclusões

O México deu passos importantes em direção à consolidação de seu sistema jurídico de proteção de dados pessoais, sob a perspectiva dos direitos humanos, o que ficou evidente com os diversos processos legislativos (como a existência de duas leis federais e 32 leis estaduais) e a assinatura e ratificação da Convenção 108 do Conselho da Europa, para citar dois exemplos.

A convicção com que se trabalhou desde a reforma constitucional do artigo 16, para reconhecer o direito à proteção de dados como um direito fundamental, foi fortalecer o sistema de direitos humanos do país com um pilar essencial: garantir o desenvolvimento adequado e saudável das pessoas no contexto da revolução tecnológica. Para isso, é necessário buscar novos espaços que ampliem a proteção de dados pessoais e ofereçam mais forças e benefícios a todos os mexicanos.

Trabalhar em busca do reconhecimento da União Europeia visa fazer parte de um sistema de direitos humanos, especificamente no componente de proteção de dados, onde se reconhecem os padrões mais exigentes na matéria em escala global.

Para o México, contar com a adequação sob a perspectiva de outros países não se concentra apenas em criar um mecanismo comercial que elimine barreiras não tarifárias ao comércio, mas o foco está em determinar se o país possui forças suficientes para garantir os direitos e liberdades fundamentais com um marco normativo robusto, instituições estatais eficazes, garantias aos titulares, entre outros, sem deixar de considerar o potencial comercial que acompanha esse tipo de processos.

Em termos do que foi exposto, consideramos que o México deve continuar avançando no fortalecimento de seu sistema de direitos humanos, por meio do reconhecimento de um nível de proteção de dados pessoais adequado, assim o México se juntaria ao conjunto de democracias com o mais alto nível de exigência no espaço de um dos direitos da personalidade (proteção de dados), com os múltiplos efeitos positivos que isso traria para o cotidiano das pessoas, dada a transversalidade dessa medida.

8 Uruguai

8.1 Introdução ao sistema uruguaio

O sistema jurídico uruguaio para transferências internacionais de dados encontra sua inspiração no Regulamento Europeu de Proteção de Dados – (EU) 2016/679 –, assim como nas normas que o precederam. Nesse sentido, vale lembrar que o Uruguai foi declarado "adequado" em 2012 (Resolução 2012/484/EU).

É relevante destacar também que o Uruguai foi o primeiro país não europeu a ratificar a Convenção 108 (10 de abril de 2013) e, até a presente data, também ratificou a Convenção 108 modernizada (5 de agosto de 2021).

Conforme o sistema uruguaio de proteção de dados pessoais, as transferências internacionais de dados são, em princípio, proibidas, e sua habilitação ocorre como uma exceção a esse princípio geral.

Nesse sentido, a lei principal de proteção de dados (Lei nº 18.331, de agosto de 2008) só permite transferências de dados pessoais para países que sejam considerados "adequados" por resolução da autoridade de proteção de dados uruguaia (a Unidade Reguladora e de Controle de Dados Pessoais, doravante, URCDP), junto com outras várias exceções estabelecidas no artigo 23 da referida lei, conforme se mencionará a seguir.

Entre as exceções que permitem a transferência de dados pessoais entre países que não são considerados adequados, podemos encontrar: o consentimento inequívoco do interessado, que deve estar devidamente documentado; as transferências realizadas para cooperar com as autoridades judiciais de outros países; a transferência de dados médicos necessários para o tratamento de uma pessoa por razões de saúde ou higiene pública; a transferência bancária ou bursátil, no que diz respeito a essas transações; as transferências de dados realizadas a partir de um registro público; as transferências de dados realizadas no âmbito de uma convenção ou tratado internacional que o Uruguai tenha assinado; as transferências de dados realizadas em cooperação entre organismos de inteligência contra o crime organizado, o tráfico ilícito de drogas e o terrorismo. Também é possível realizar transferências internacionais de dados se elas forem feitas em cumprimento de um contrato com o interessado (para a execução do contrato ou para a execução de medidas pré-contratuais a pedido do inte-

ressado), ou se a transferência for necessária para celebrar ou executar um contrato entre o controlador e um terceiro, desde que seja no interesse do interessado; se for necessário ou obrigatório para a salvaguarda de um interesse público importante, ou para o reconhecimento, exercício ou defesa de um direito em um processo judicial; ou no caso em que a transferência seja necessária para a salvaguarda do interesse vital do interessado.

8.2 Autorização à Unidade Reguladora e de Controle de Dados Pessoais (URCDP) para realizar as transferências internacionais

No entanto, mesmo que o país de destino não forneça padrões de "adequação" e a transferência não esteja dentro das exceções legais, o controlador da base de dados pode solicitar autorização à URCDP para realizar as transferências internacionais de dados, oferecendo garantias suficientes quanto à proteção da vida privada, dos direitos e liberdades fundamentais das pessoas, assim como quanto ao exercício dos respectivos direitos.

Para conceder a autorização mencionada, que é competência da Unidade Reguladora, serão considerados a adoção de cláusulas contratuais, a localização do controlador do tratamento (e se o país onde está localizado adotou alguma normativa de proteção de dados), bem como a autocertificação fornecida pelo órgão americano de controle FTC (Federal Trade Commission dos Estados Unidos da América).

Em 2021, o regime uruguaio de proteção de dados foi impactado pelo caso "Schrems II" (C-311/18) e pela decisão do TJUE, de 16 de julho de 2020, como ocorreu em outras partes do mundo. Como consequência, a URCDP anunciou algumas mudanças no regime de proteção de dados em relação às transferências internacionais de dados pessoais.

8.3 As resoluções URCDP nºs 23/2021[79], 63/023[80]e 70/023[81]

A Resolução URCDP nº 23/2021 fez alguns ajustes em relação aos países considerados "adequados" para as transferências internacionais de dados, removendo da lista as transferências realizadas sob o programa *Privacy Shield* entre a União Europeia e os Estados Unidos da América. A URCDP também tomou outras medidas complementares, como estabelecer um prazo para a adequação dos contratos existentes realizados sob o programa *Privacy Shield*.

Além disso, estabeleceu quais são os países considerados adequados para as transferências de dados pessoais: países da UE e do Acordo EEE, Andorra, Argentina, o setor privado do Canadá, Guernsey, Ilha de Man, Ilhas Faroe, Israel, Japão, Jersey, Nova Zelândia, Reino Unido, Irlanda do Norte e Suíça. A eliminação do *Privacy Shield* da lista foi a mudança mais relevante.

A ideia explícita por trás dessa decisão foi manter o país atualizado para cumprir com os Padrões Internacionais de Proteção de Dados da Rede Ibero-Americana de Proteção de Dados e o RGPD, permitindo que o Uruguai continue sendo "adequado" de acordo com os padrões europeus.

Posteriormente, em 2023, a Resolução URCDP nº 63/023 voltou a modificar a lista de países adequados, considerando a Decisão de Execução (UE) 2023/1795 da Comissão Europeia, incorporando, além dos mencionados anteriormente, as transferências realizadas para as entidades sujeitas à Lei de Proteção da Informação Pessoal da República da Coreia e para organizações incluídas na "Lista do Marco de Privacidade de Dados" publicada pelo Departamento de Comércio dos Estados Unidos da América

79 URUGUAI. **Unidad Reguladora y de Control de Datos Personales. Resolución Nº 23/021.** Montevidéu, 2021. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-23021.

80 URUGUAI. **Unidad Reguladora y de Control de Datos Personales. Resolución Nº 63/023.** Montevidéu, 2023. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-63023#:~:text=La%20pertinencia%20de%20actualizar%20la,11%20de%20agosto%20de%202008.

81 URUGUAI. **Unidad Reguladora y de Control de Datos Personales. Resolución Nº 70/023.** Montevidéu, 2023. Diponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-7002.

(que havia sido removida em 2021), dentro das limitações e salvaguardas estabelecidas nas decisões correspondentes.

A Resolução URCDP nº 70/023 acrescenta que, quando forem realizadas transferências para organizações incluídas no Marco de Privacidade UE-EUA, os controladores e operadores deverão apresentar, à URCDP, no momento da inscrição da base de dados ou antes da transferência, uma declaração expressa na qual a organização importadora declare ter estendido a aplicação das salvaguardas desse marco de privacidade aos dados transferidos do Uruguai. Caso essa declaração não seja realizada, a transferência poderá ser feita com base em cláusulas contratuais que tenham a prévia autorização da URCDP, ou em alguma das exceções previstas legalmente.

De acordo com o artigo 13 da Lei, deve-se informar ao titular dos dados a existência de transferências internacionais de dados. Além disso, a Resolução URCDP nº 70/023 impõe aos controladores e operadores que realizem transferências internacionais de dados a obrigação de comunicar aos titulares dos dados: *i)* o destino dos seus dados; *ii)* o papel do importador; *iii)* o prazo da transferência; *iv)* a base de legitimação; e *iv)* as operações de tratamento realizadas pelo importador.

A mesma resolução concede aos controladores e operadores um prazo de 6 meses para adotar suas políticas de privacidade.

8.4 A resolução URCDP nº 41/21[82]

A Resolução URCDP nº 41/2021 disponibiliza aos controladores e operadores pelo tratamento um guia sobre as cláusulas de redação de um contrato de transferência de dados, servindo como exemplo de boas práticas e como prova de conformidade exigida pelo artigo 23 da Lei nº 18.331 para os casos em que a autorização da URCDP para realizar a transferência internacional de dados é necessária.

As transferências internacionais de dados para países considerados "não adequados" pela URCDP devem ser precedidas de uma análise de risco e impacto dessa transferência (artigo 6, alínea f do Decreto regulamentar nº 64/020, de fevereiro de 2020). A guia contém algumas estipulações

82 URUGUAI. **Unidad Reguladora y de Control de Datos Personales. Resolución N. 41/021.** Montevidéu, 2021. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-41021.

consideradas de suma importância, que constituem o conteúdo mínimo de cada contrato de transferência de dados.

Ela inclui cláusulas gerais e específicas. As cláusulas gerais estabelecem as disposições que devem estar em todo contrato internacional de transferência de dados, enquanto as específicas detalham o conteúdo necessário de acordo com as partes que assinam o contrato (controlador-controlador, controlador-operador, operador-operador). As cláusulas gerais são requerimentos baseados na necessidade de que certas informações estejam explicitamente indicadas nos termos do contrato, embora algumas soluções particulares também sejam obrigatórias.

Embora o texto da resolução não tenha caráter obrigatório para quem a subscreve, alguns termos dela denotam obrigatoriedade. Este é o caso da finalidade da cessão, que deve estar claramente estabelecida no contrato.

Além disso, deve conter a normativa aplicável e definir os termos mais comuns, estabelecendo também o direito de informação do titular dos dados, conforme regulamentado pelo artigo 13 da Lei nº 18.331, que especifica as informações que devem ser fornecidas ao interessado quando os dados são coletados, incluindo a identidade do operador do tratamento e dos suboperadores (se aplicável). Essas informações devem estar permanentemente disponíveis ou ser fornecidas a pedido do interessado.

Em todo caso, o contrato deve estipular que – em caso de descumprimento – a autoridade administrativa competente será a uruguaia, com exceção dos casos em que o importador esteja sujeito a uma autoridade reguladora homônima no país de destino.

A análise de impacto obrigatória (artigo 6 *f* do Decreto nº 64/020) deve ser anexada ao contrato como prova da devida diligência em segurança e privacidade dos dados.

Com relação às informações que devem ser explicitamente indicadas no contrato, os dados específicos, transferidos para o terceiro país, devem ser detalhados. Caso haja dados sensíveis, deve-se detalhar o conteúdo e o propósito da transferência de cada dado.

Devem ser indicadas as operações de tratamento a serem realizadas, bem como as medidas operacionais e de segurança necessárias para cumprir com o princípio de segurança dos dados e de responsabilidade proativa dos artigos 10 e 12 da Lei nº 18.331 (na sua nova redação pelo artigo 39 da Lei nº 19.670 e Decreto nº 64/020).

Se houver transferência de dados posterior, também devem ser estabelecidas as condições sob as quais os dados serão transferidos para outra parte.

Sobre a resolução de disputas, as partes podem estipular qualquer mecanismo desde que não altere os direitos do titular dos dados, não contrarie as leis aplicáveis, não modifique as operações de tratamento de interesse do titular dos dados, nem estabeleça uma retenção indevida de informações, que deve ser eliminada conforme a lei aplicável.

Sobre a resolução de disputas, as partes podem estipular qualquer mecanismo desde que não altere os direitos do titular dos dados, não contrarie as leis aplicáveis, não modifique as operações de tratamento de interesse do titular dos dados, nem estabeleça uma retenção indevida de informações, que deve ser eliminada conforme a lei aplicável.

A guia também exige que o contrato estabeleça o conteúdo das obrigações de confidencialidade assumidas pelo pessoal do importador e do exportador, assim como que apenas as autoridades de controle do país de destino possam acessar a base de dados com uma ordem judicial e sempre dentro do marco legal vigente que garanta os direitos dos titulares dos dados, acessando apenas os dados estritamente necessários para cumprir a ordem judicial.

As cláusulas específicas abordam as bases legais para essa transferência em particular e todas as posteriores, com especial atenção à responsabilidade de cada parte pelos danos causados aos direitos do titular dos dados.

Embora as cláusulas sejam obrigatórias para as transferências de dados realizadas para países que "não são adequados" segundo a autoridade uruguaia, a resolução incentiva todos os controladores a considerar essas cláusulas em todo tipo de transferência internacional de dados, quando pertinente.

8.5 A resolução URCDP nº 50/22[83]

Além da Resolução URCDP nº 41/2021, cabe mencionar a Resolução URCDP nº 50/2022, que recomenda o uso das cláusulas da Rede Ibero-Americana de Proteção de Dados para transferências no âmbito do artigo 23 da Lei nº 18.331, com as adaptações necessárias à normativa nacional. A resolução esclarece que seu uso não exclui a autorização prévia da Unidade.

83 URUGUAI. *Unidad Reguladora y de Control de Datos Personales. Resolución N. 50/022*. Montevidéu, 2022. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-50022.

Além disso, a URCDP adotou uma abordagem que visa facilitar o processo de solicitação de autorização, pré-analisando contratos de provedores de serviços na internet (como Microsoft e AWS), considerando a adequação dessas cláusulas à normativa uruguaia (ver as Resoluções URCDP nº 11/2020 e nº 42/2022).

Isso não exclui a solicitação de autorização da Unidade, embora para facilitar esse processo a controladores e operadores, foi disponibilizado um mecanismo totalmente online, disponível no site da URCDP.

8.6 Conclusões

As novas resoluções do Uruguai estabelecem novas obrigações para os envolvidos em transferências internacionais de dados, estruturando um sistema mais complexo e oneroso, especialmente para as empresas, mas que permite ao país manter-se alinhado ao sistema europeu de proteção de dados pessoais. A adaptação aos padrões pré-acordados pelo Estado uruguaio em matéria de proteção de dados pessoais demonstra um compromisso com a cooperação internacional, o qual é aceito e especialmente valorizado pelos diversos atores com diferentes interesses envolvidos.

9 Considerações finais

9.1 Tabela comparativa dos países analisados

A tabela comparativa mostra um resumo das regras vigentes em cada um dos países que expusemos nos itens anteriores.

	Argentina	**Brasil**	**Colômbia**	**México**	**Uruguai**
Normas aplicáveis	Lei nº 25.326, artigo 12 e Disposição 60.	LGPD, artigos 33/34.	Lei nº 1.581 de 2012, artigo 26.	Lei federal, artigos 36/37.	Lei nº 18.331, artigo 23. Resolução URCDP nº 41/021 e 50/2022

Prevê a possibilidade de que a autoridade de dados ou outra autoridade pública declare ou liste outros países com nível adequado de proteção de dados?	Sim	Sim	Sim	Não	Sim
Permite que o controlador do tratamento avalie se o país de destino da informação tem um nível adequado de proteção de dados?	Sim	Sim	Sim	Não	Não
Consagra a possibilidade de que os Estados pactuem acordos *sui generis* para transferir dados entre eles, tal como acontece na Europa e nos Estados Unidos?	Não	Sim	Sim	Não	Não
Permite que se legitime a transferência internacional de dados com a autorização/ consentimento do titular dos dados?	Sim	Sim	Sim	Sim	Sim
A autorização do titular deve cumprir requisitos adicionais ou especiais para realizar transferências internacionais de dados?	Não	Não	Não	Sim	Não
Consagra expressamente as cláusulas-padrão contratuais como alternativa para transferir dados a outros países?	Sim	Sim	Não	Sim	Sim
Consagra expressamente as normas corporativas vinculantes como alternativa para transferir dados a outros países?	Sim	Sim	Sim	Sim	Não
Prevê a figura da coleta internacional de dados pessoais?	Não	Não	Sim	Não	Não

Foi reconhecido pela UE como país adequado?	Sim	Não	Não	Não	Sim
Foi reconhecido por outro(s) país(es) ou organização diferente da UE como país com nível adequado?	Sim	Não	Sim	Sim	Sim
Existem casos judiciais sobre esta temática?	Não	Não	Não	Não	Não
Aprovou cláusulas-padrão contratuais para transferências?	Sim	Não	Não	Não	Sim
Aprovou SCC da RIPD?	Sim	Não	Não	Não	Sim
CBPR?	Não	Não	Não	Sim	Não

A partir da análise dos capítulos anteriores e do que foi apresentado na tabela, podemos esboçar as seguintes conclusões:

- **Todos** os países analisados oferecem a possibilidade de que a autoridade de dados ou outra autoridade pública declare ou liste outros países com um nível adequado de proteção de dados;
- Três dos países deste estudo permitem que o controlador do tratamento avalie se o país de destino da informação possui um nível adequado de proteção de dados;
- **Todos** os países deste estudo permitem que a transferência internacional de dados seja legitimada com a autorização do titular dos dados;
- **Todos** os países analisados permitem as cláusulas contratuais como alternativa para transferir dados pessoais a outros países. Argentina, Peru e Uruguai aprovaram as cláusulas-padrão da Rede Ibero-Americana;
- Três países (Argentina, Colômbia e Brasil) contemplam expressamente as normas corporativas vinculantes como alternativa para transferir dados a outros países;

- Só um país (Colômbia) prevê a figura da coleta internacional de dados pessoais;
- Só um país (México) contempla a possibilidade de usar CBPR devido à sua participação no tratado de livre comércio entre Estados Unidos da América, Canadá e México (TMEC) e aos compromissos internacionais que assumiu;
- Só dois países (Argentina e Uruguai) foram reconhecidos como adequados pela UE nas últimas duas décadas;
- Argentina, Colômbia, México e Uruguai foram reconhecidos por outros países e organizações diferentes da UE como países com nível adequado de proteção;
- América Latina realizou os seguintes reconhecimentos de adequação:
    - Argentina reconheceu como adequados todos os países que em 2016 a UE havia reconhecido como adequados, e somou a essa lista o Reino Unido em 2018, em decorrência do Brexit;
    - Colômbia reconheceu como países com nível adequado: Alemanha; Austrália, Áustria; Bélgica; Bulgária; Chipre; Costa Rica; Croácia; Dinamarca; Eslováquia; Eslovênia; Estônia; Espanha; Estados Unidos da 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; Suécia; e os países que foram declarados com nível adequado de proteção pela Comissão Europeia (Suíça; Canadá; Argentina, Guernsey, Ilha de Man, Jersey, Ilhas Faroé, Andorra, Israel, Uruguai, Nova Zelândia e Japão).
    - Uruguai reconheceu como adequados todos os países que a UE reconheceu como adequados.

9.2 Desafios atuais na América Latina

As transferências internacionais de dados enfrentam vários desafios. Considerando sua importância na economia digital, tornam-se práticas imprescindíveis, que devem cumprir com os padrões de qualidade e segurança para os usuários, levando em conta que, em alguns casos, sua implementação é complexa devido às diferenças nas regulamentações em cada país e à incessante inovação tecnológica que, dia após dia, oferece novas formas de comercializar produtos e serviços.

A seguir, são listados alguns desafios que surgem como áreas de oportunidade para a transferência eficaz e segura de dados:

1. Proteção de dados e privacidade: Um dos principais desafios é garantir a proteção e privacidade dos dados durante as transferências internacionais. Os dados podem estar sujeitos a diferentes leis e regulamentos em cada país, o que gera discrepâncias no nível de proteção e dificulta a garantia da privacidade das pessoas.

2. Jurisdição e marcos regulatórios: As transferências internacionais de dados são influenciadas por diferentes jurisdições e marcos regulatórios em diversos países. Cada país pode ter leis e regulamentações diferentes em relação à proteção de dados, o que pode criar desafios para cumprir os requisitos legais e respeitar os direitos de privacidade em diferentes contextos.

3. Segurança dos dados: As transferências internacionais de dados podem apresentar riscos de segurança, pois os dados podem estar expostos a ameaças cibernéticas, pirataria ou interceptação não autorizada durante o processo de transferência. A implementação de medidas de segurança robustas é essencial para proteger os dados durante a transferência e o armazenamento.

4. Consentimento informado: Obter o consentimento informado das pessoas para transferir seus dados pessoais no âmbito internacional pode ser um desafio. As pessoas podem não estar totalmente cientes de como seus dados serão usa-

dos em outros países ou dos riscos associados. Garantir um consentimento válido e claro torna-se um desafio importante.

5. Transferências para países com níveis de proteção inadequados: Alguns países podem ter níveis de proteção de dados considerados inadequados em comparação com os padrões internacionais. A transferência de dados pessoais para esses países pode apresentar riscos adicionais para a privacidade e segurança dos dados.

6. Transparência e prestação de contas: As organizações devem ser transparentes sobre como os dados pessoais são transferidos, armazenados e utilizados no contexto das transferências internacionais. Além disso, devem assumir a responsabilidade de garantir o cumprimento das normas e padrões aplicáveis.

Para enfrentar esses desafios, foram estabelecidos marcos legais e mecanismos de autorregulação, como acordos de transferência de dados e padrões de segurança, para garantir uma proteção adequada dos dados e o respeito aos direitos de privacidade nas transferências internacionais de dados pessoais. Uma prática que devemos incentivar é a adoção de esquemas de autorregulação vinculante, bem como a adoção de instrumentos jurídicos específicos, como cláusulas-padrão ou normas corporativas vinculantes (BCR, na sigla em inglês), entre outros.

9.3 Algumas ideias para o desenvolvimento de mecanismos de adequação "latino-americanos"

Na América Latina, é necessário desenvolver um marco regional adequado para o reconhecimento de adequação das jurisdições locais, a fim de permitir o livre fluxo de dados dentro de um quadro que proteja os direitos de proteção de dados pessoais.

Isso poderia ocorrer de diferentes maneiras, entre elas, as possibilidades que descrevemos a seguir:

a) Reconhecimento com base nas legislações de dados pessoais vigentes em cada jurisdição, utilizando um *checklist* baseado nos padrões ibero-americanos desenvolvidos pela RIPD como

uma espécie de "quadro geral" para o reconhecimento de adequação. Este *checklist* poderia ser elaborado pela Rede Ibero-Americana por meio de um acordo conjunto entre várias autoridades de proteção de dados pessoais da região (e ir somando as que queiram participar) ou até mesmo em escala regional para os membros do Mercosul ou do Pacto Andino.

b) Considerar a existência e aplicação de tratados vigentes sobre direitos humanos (como a Convenção Americana sobre Direitos Humanos) e sobre proteção de dados pessoais (como o Convênio 108 original ou o Convênio 108+) na jurisdição de destino da transferência de dados.

c) Desenvolver, promover e implementar o uso de cláusulas-padrão contratuais para toda a região. Nesse sentido, a RIPD elaborou uma primeira versão das cláusulas-padrão contratuais para transferências a controladores e a operadores de dados e um Guia de implementação delas. Por ora, apenas Peru e Uruguai adotaram esse modelo, e outros países estão analisando. Mas ainda há muito a ser feito, como, por exemplo, gerar mais módulos alternativos, como fez a UE ao aprovar quatro modelos, e não apenas dois, ou redigir um modelo de SCC+ para a América Latina, compatível com o modelo da UE. Essa opção será explorada no capítulo 2 deste volume.

d) Elaborar um tratado regional de proteção de dados pessoais no âmbito latino-americano (por exemplo, no âmbito da Organização dos Estados Americanos, OEA, e seguindo os princípios atualizados de 2021) que estabeleça como princípio geral que os países-membros, em virtude dos compromissos assumidos nesse tratado, possuem um nível adequado de proteção de dados pessoais para fins de livre fluxo de dados pessoais dentro dos países-membros e que fomente a cooperação direta entre as agências de dados pessoais. Essa opção será explorada no capítulo 3 deste volume.

e) Desenvolver e promover o uso de *binding corporate rules* para toda a região por meio da RIPD ou através de um acordo de reconhecimento mútuo direto entre autoridades de pro-

teção de dados pessoais, com um canal compartilhado entre todas para designar uma autoridade de origem (aquela que recebe o pedido de aprovação de BCR e compila comentários de todas as agências) e um procedimento interno de aprovação regional de BCR para toda a América Latina.

f) "Pontes": Considerar a possibilidade de reconhecimento mútuo entre diferentes jurisdições, criando equivalência com outras ferramentas ou cláusulas-padrão vigentes em outras regiões (BRICS, Mercosul, Comunidade Andina, APEC, ASEAN, UE, Fórum de Autoridades de Privacidade da Ásia-Pacífico – APPA Fórum – e Conselho da Europa) por meio de "pontes" ou acordos regionais onde um bloco reconheça as ferramentas de transferência internacional usadas por outro bloco. Isso evitaria os reconhecimentos unilaterais que acabam criando um "campo minado" para o livre fluxo de dados pessoais.

g) Explorar a possibilidade de desenvolver infraestruturas públicas digitais para a gestão de dados pessoais, que permitam traduzir em software os dispositivos normativos ou as disposições contratuais das cláusulas-padrão. Tal estratégia poderia se inspirar na experiência da Índia, onde, há vários anos, a gestão de dados pessoais tem sido facilitada por meio de um tipo de infraestrutura pública digital chamada "*Data Empowerment and Protection Architecture*". Essa opção é particularmente interessante porque é autoexecutável, ou seja, permitiria adicionar uma camada de software regulando diretamente na arquitetura lógica como os dados poderiam ser transferidos. No entanto, essa opção ainda precisa ser estudada mais a fundo para entender como seria implementada concretamente. Nesse sentido, essa opção ainda não é explorada neste trabalho, sendo objeto de investigação futura.

Anexo A – Regulamento de Transferência Internacional de Dados e o Conteúdo das Cláusulas-Padrão Contratuais Estabelecidas pela ANPD

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 23/08/2024 | Edição: 163 | Seção: 1 | Página: 123

Órgão: Ministério da Justiça e Segurança Pública/Autoridade Nacional de Proteção de Dados/Conselho Diretor

RESOLUÇÃO CD/ANPD Nº 19, DE 23 DE AGOSTO DE 2024

Aprova o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais.

O CONSELHO DIRETOR DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD), com base nas competências previstas no art. 55-J, inciso XIII, da Lei nº 13.709, de 14 de agosto de 2018, no art.2º, inciso XIII, do Anexo I, do Decreto nº 10.474, de 26 de agosto de 2020, no art. 5º, inciso I, do Regimento Interno da ANPD, e tendo em vista a deliberação tomada no processo nº 00261.000968/2021- 06, resolve:

Art. 1º Esta Resolução aprova, na forma dos Anexos I e II, o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais, nos termos do art. 33, incisos I e II, alíneas 'a', 'b' e 'c', art. 34, art. 35, caput e §§ 1º, 2º e 5º, e art. 36 da Lei nº 13.709, de 14 de agosto de 2018.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

Parágrafo único. Os agentes de tratamento que utilizam cláusulas contratuais para realizar transferências internacionais de dados deverão incorporar as cláusulas-padrão contratuais aprovadas pela ANPD aos seus respectivos instrumentos contratuais, no prazo de até 12 (doze) meses, contados da data de publicação desta Resolução.

WALDEMAR GONÇALVES ORTUNHO JUNIOR
Diretor-Presidente

Anexo B – Regulamento de Transferência Internacional de Dados

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Seção I
Objetivo e Escopo

Art. 1º Este Regulamento estabelece os procedimentos e as regras aplicáveis às operações de transferência internacional de dados:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na Lei nº 13.709, de 14 de agosto de 2018, mediante reconhecimento da adequação pela ANPD; ou

II - quando controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na Lei nº 13.709, de 14 de agosto de 2018, na forma de:

a. cláusulas contratuais específicas para determinada transferência;

b. cláusulas-padrão contratuais; ou

c. normas corporativas globais.

Parágrafo único. O disposto neste Regulamento não exclui a possibilidade da realização de transferência internacional de dados com base nos demais mecanismos previstos no art. 33 da Lei nº 13.709, de 14 de agosto de 2018, que não dependam de regulamentação, desde que atendidas as especificidades do caso concreto e os requisitos legais aplicáveis.

Seção II
Diretrizes

Art. 2º A transferência internacional de dados será realizada em conformidade com o disposto na Lei nº 13.709, de 14 de agosto de 2018, e neste Regulamento, observadas as seguintes diretrizes:

I - garantia de cumprimento dos princípios, dos direitos do titular e de nível de proteção equivalente ao previsto na legislação nacional, independentemente do país onde estejam localizados os dados pessoais objeto da transferência, inclusive após o término do tratamento e nas hipóteses de transferências posteriores;

II - adoção de procedimentos simples, preferencialmente interoperáveis, e compatíveis com normas e boas práticas internacionais;

III - promoção do livre fluxo transfronteiriço de dados com confiança e do desenvolvimento social, econômico e tecnológico, com observância aos direitos dos titulares;

IV - responsabilização e prestação de contas, mediante a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento dos princípios dos direitos do titular e do regime de proteção de dados pessoais previstos na Lei nº 13.709, de 14 de agosto de 2018, inclusive, da eficácia dessas medidas;

I- implementação de medidas efetivas de transparência, que assegurem o fornecimento aos titulares de informações claras, precisas e facilmente acessíveis sobre a realização da transferência, observados os segredos comercial e industrial; e

II - adoção de boas práticas e de medidas de prevenção e segurança apropriadas e compatíveis com a natureza dos dados pessoais tratados, a finalidade do tratamento e os riscos envolvidos na operação.

CAPÍTULO II
DAS DEFINIÇÕES

Art. 3º Para efeitos deste Regulamento são adotadas as seguintes definições:

I - exportador: agente de tratamento, localizado no território nacional ou em país estrangeiro, que transfere dados pessoais para importador;

II - importador: agente de tratamento, localizado em país estrangeiro ou que seja organismo internacional, que recebe dados pessoais transferidos por exportador;

III - transferência: operação de tratamento por meio da qual um agente de tratamento transmite, compartilha ou disponibiliza acesso a dados pessoais a outro agente de tratamento;

IV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

V - coleta internacional de dados: coleta de dados pessoais do titular efetuada diretamente pelo agente de tratamento localizado no exterior;

VI - grupo ou conglomerado de empresas: conjunto de empresas de fato ou de direito com personalidades jurídicas próprias, sob direção, controle ou administração de uma pessoa natural ou jurídica ou ainda grupo de pessoas que detêm, isolada ou conjuntamente, poder de controle sobre as demais, desde que demonstrado interesse integrado, efetiva comunhão de interesses e atuação conjunta das empresas dele integrantes;

VII - entidade responsável: 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 ou conglomerado de empresas com sede em outro país;

VIII - mecanismos de transferência internacional de dados: hipóteses previstas nos incisos I a IX do art. 33 da Lei nº 13.709, de 14 de agosto de 2018, que autorizam uma transferência internacional de dados;

IX - organismo internacional: organização regida pelo direito internacional público, incluindo seus órgãos subordinados ou qualquer outro órgão criado mediante acordo firmado entre dois ou mais países; e

X - medidas de segurança: medidas técnicas e administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

CAPÍTULO III
TRANSFERÊNCIA INTERNACIONAL DE DADOS

Seção I
Requisitos Gerais

Art. 4º Cabe ao controlador verificar, nos termos da Lei nº 13.709, de 14 de agosto de 2018, e deste Regulamento, se a operação de tratamento:

I - caracteriza transferência internacional de dados;

I - submete-se à legislação nacional de proteção de dados pessoais; e

III - está amparada em hipótese legal e em mecanismo de transferência internacional válidos.

§ 1º O operador prestará auxílio ao controlador mediante o fornecimento das informações de que dispuser e que se demonstrarem necessárias para o atendimento ao disposto no caput deste artigo.

§ 2º O controlador e o operador deverão adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e da eficácia dessas medidas, de forma compatível com o grau de risco do tratamento e com o mecanismo de transferência internacional utilizado.

Seção II
Caracterização da Transferência Internacional de Dados

Art. 5º A transferência internacional de dados será caracterizada quando o exportador transferir dados pessoais para o importador.

Art. 6º A coleta internacional de dados não caracteriza transferência internacional de dados.

Parágrafo único. A coleta internacional de dados observará as disposições da Lei nº 13.709, de 14 de agosto de 2018, quando verificada uma das hipóteses indicadas no art. 3º da Lei.

Seção III
Aplicação da Legislação Nacional de Proteção de Dados Pessoais

Art. 7º A transferência internacional de dados deverá observar as disposições da Lei nº 13.709, de 14 de agosto de 2018, e deste Regulamento, quando:

I - a operação de tratamento for realizada no território nacional, ressalvado o disposto no inciso IV do caput do art. 4º da Lei nº 13.709, de 14 de agosto de 2018, e observado o disposto no art. 8º deste Regulamento;

II - a atividade de tratamento tiver por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou

III - os dados pessoais, objeto do tratamento, forem coletados no território nacional.

Parágrafo único. A aplicação da legislação nacional à transferência internacional de dados independe do meio utilizado para sua realização, do país de sede dos agentes de tratamento ou do país onde estejam localizados os dados.

Art. 8º Aplica-se a Lei nº 13.709, de 14 de agosto de 2018, aos dados pessoais provenientes do exterior sempre que estes sejam objeto de tratamento no território nacional.

§ 1º A Lei nº 13.709, de 14 de agosto de 2018, não se aplica aos dados pessoais provenientes do exterior somente quando ocorrer:

I - trânsito de dados pessoais, sem a ocorrência de comunicação ou uso compartilhado de dados com agente de tratamento situado em território nacional; ou

II - retorno dos dados pessoais, objeto de tratamento no território nacional, exclusivamente ao país ou organismo internacional de proveniência, desde que:

a. o país ou organismo internacional de proveniência proporcione grau de proteção de dados pessoais adequado, reconhecido por decisão da ANPD;

b. a legislação do país ou as normas aplicáveis ao organismo internacional de proveniência se apliquem à operação realizada; e

c. a situação específica e excepcional de não aplicação da Lei nº 13.709, de 14 de agosto de 2018, esteja expressamente prevista na decisão de adequação referida na alínea "a".

§ 2º Para fins do inciso II do § 1º, a decisão de adequação emitida pela ANPD não excepcionará a aplicação da Lei nº 13.709, de 14 de agosto de 2018, em situações que possam violar ou colocar em risco a observância dos princípios gerais de proteção de dados pessoais e os direitos dos titulares previstos na legislação nacional.

§ 3º A não aplicação da Lei nº 13.709, de 14 de agosto de 2018, nas hipóteses previstas neste artigo não afasta a necessidade de observância de outras leis ou regulamentos, especialmente os que dispõem sobre inviolabilidade e sigilo das comunicações, requisitos técnicos e de segurança e acesso a dados por autoridades públicas.

Seção IV
Hipótese Legal e Mecanismo de Transferência

Art. 9º A transferência internacional de dados 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, e desde que amparada em:

I - uma das hipóteses legais previstas no art. 7º ou no art. 11 da Lei nº 13.709, de 14 de agosto de 2018; e

II - um dos seguintes mecanismos válidos de realização da transferência internacional:

a) para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na Lei nº 13.709, de 14 de agosto de 2018, e em normas complementares, conforme reconhecido por decisão de adequação emitida pela ANPD;

b cláusulas-padrão contratuais, normas corporativas globais ou cláusulas contratuais específicas, na forma deste Regulamento; ou

c) nas hipóteses previstas nos incisos II, "d", e III a IX do art. 33 da Lei nº 13.709, de 14 de agosto de 2018.

Parágrafo único. A transferência internacional de dados deverá se limitar ao mínimo necessário para o alcance de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

CAPÍTULO IV
DECISÃO DE ADEQUAÇÃO

Seção I
Disposições Gerais

Art. 10. A ANPD poderá reconhecer, mediante decisão de adequação, a equivalência do nível de proteção de dados pessoais de país estrangeiro ou de organismo internacional com a legislação nacional de proteção de dados pessoais, observado o disposto na Lei nº 13.709, de 14 de agosto de 2018, e neste Regulamento.

Seção II
Critérios para Avaliação do Nível de Proteção de Dados Pessoais

Art. 11. A avaliação do nível de proteção de dados pessoais de país estrangeiro ou de organismo internacional levará em consideração:

A - as normas gerais e setoriais em vigor com impactos sobre a proteção de dados pessoais no país de destino ou no organismo internacional;

B - a natureza dos dados;

C - a observância dos princípios gerais de proteção de dados pessoais e dos direitos dos titulares previstos na Lei nº 13.709, de 14 de agosto de 2018;

D - a adoção de medidas de segurança adequadas para minimizar impactos às liberdades civis e aos direitos fundamentais dos titulares;

E - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e

F - outras circunstâncias específicas relativas à transferência.

§ 1º A avaliação das normas mencionadas no inciso I do caput deste artigo será limitada à legislação diretamente aplicável ou que gere impactos relevantes sobre o tratamento de dados pessoais e sobre os direitos dos titulares.

§ 2º Para fins do disposto nos incisos III e IV do caput deste artigo, será avaliado se a legislação local estabelece aos agentes de tratamento obrigações de implementação de medidas de segurança adequadas, considerando a natureza dos dados e os riscos envolvidos no tratamento, entre

outros fatores relevantes, em conformidade com os parâmetros estabelecidos na Lei nº 13.709, de 14 de agosto de 2018.

§ 3º Para fins do disposto no inciso V do caput deste artigo, serão consideradas, entre outras garantias institucionais relevantes, a existência e o efetivo funcionamento de um órgão regulador independente, com competência para assegurar o cumprimento das normas de proteção de dados e garantir os direitos dos titulares.

Art. 12. Para a avaliação do nível de proteção de dados pessoais, também serão levados em consideração:

I - os riscos e os benefícios proporcionados pela decisão de adequação, considerando, entre outros aspectos, a garantia dos princípios, dos direitos do titular e do regime de proteção de dados previstos na Lei nº 13.709, de 14 de agosto de 2018; e

II - os impactos da decisão sobre o fluxo internacional de dados, as relações diplomáticas, o comércio internacional e a cooperação internacional do Brasil com outros países e organismos internacionais.

Parágrafo único. A ANPD priorizará a avaliação do nível de proteção de dados de países estrangeiros ou organismos internacionais que garantam tratamento recíproco ao Brasil e cujo reconhecimento de adequação viabilize a ampliação do livre fluxo de transferências internacionais de dados pessoais entre os países e organismos internacionais.

Seção III
Emissão de Decisão de Adequação

Art. 13. O procedimento para emissão de decisão de adequação:

I - poderá ser instaurado por decisão do Conselho Diretor, de ofício ou após solicitação das pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011;

II - será instruído pela área técnica competente, nos termos do Regimento Interno da ANPD, que se manifestará sobre o mérito da decisão, indicando, se for o caso, as condicionantes a serem observadas; e

III - após a manifestação da Procuradoria Federal Especializada, será objeto de deliberação final pelo Conselho Diretor, na forma do Regimento Interno da ANPD.

§ 1º Os órgãos e entidades da Administração Pública com competências afetas ao tema poderão ser cientificados da instauração do processo, sendo-lhes facultada a apresentação de manifestação, no âmbito de suas competências legais.

§ 2º A decisão de adequação será proferida por Resolução do Conselho Diretor e publicada na página da ANPD na Internet.

Art. 14. O processo instaurado no âmbito da ANPD com vistas à elaboração de documentos, fornecimento de informações e quaisquer outros atos relativos ao reconhecimento do Brasil como país adequado por outro país ou organismo internacional observarão os procedimentos descritos no art. 13 deste Regulamento.

CAPÍTULO V
CLÁUSULAS-PADRÃO CONTRATUAIS

Seção I
Disposições Gerais

Art. 15. As cláusulas-padrão contratuais, elaboradas e aprovadas pela ANPD na forma do Anexo II, estabelecem garantias mínimas e condições válidas para a realização de transferências internacionais de dados baseadas no inciso II, alínea "b", do art. 33 da Lei nº 13.709, de 14 de agosto de 2018.

Parágrafo único. As cláusulas-padrão contratuais visam garantir a adoção das salvaguardas adequadas para o cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na Lei nº 13.709, de 14 de agosto de 2018, incluindo as determinações da ANPD.

Art. 16. A validade da transferência internacional de dados, quando amparada na adoção das cláusulas-padrão, pressupõe a adoção integral e sem alteração do texto disponibilizado no Anexo II, mediante instrumento contratual firmado entre o exportador e o importador.

§ 1º As cláusulas-padrão contratuais poderão integrar:

I - contrato celebrado para reger especificamente transferências internacionais de dados;

II - contrato com objeto mais amplo, inclusive mediante a assinatura de termo aditivo pelo exportador e pelo importador envolvidos na operação de transferência internacional de dados.

§ 2º As demais disposições, previstas no instrumento contratual ou em contratos coligados firmados pelas partes, não poderão excluir, modificar ou contrariar, direta ou indiretamente, o disposto nas cláusulas-padrão contratuais.

§ 3º Na hipótese do inciso II do § 1º deste artigo, as Seções I, II e III do Anexo II deverão figurar como documento anexo do instrumento contratual assinado entre exportador e importador.

Seção II
Medidas de Transparência

Art. 17. O controlador deverá disponibilizar ao titular, em caso de solicitação, a íntegra das cláusulas utilizadas para a realização da transferência internacional de dados, observados os segredos comercial e industrial.

§ 1º O prazo para atendimento da solicitação é de 15 (quinze) dias, ressalvada a hipótese de prazo distinto estabelecido em regulamentação específica da ANPD.

§ 2º O controlador deverá ainda publicar em sua página na Internet documento contendo informações em língua portuguesa, em linguagem simples, clara, precisa e acessível sobre a realização da transferência internacional de dados, incluindo, pelo menos, informações sobre:

I - a forma, a duração e a finalidade específica da transferência internacional;

II - o país de destino dos dados transferidos;

III - a identificação e os contatos do controlador;

IV - o uso compartilhado de dados pelo controlador e a finalidade;

V - as responsabilidades dos agentes que realizarão o tratamento e as medidas de segurança adotadas; e

VI - 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.

§ 3º O documento referido no § 2º poderá ser disponibilizado em página específica ou integrado, de forma destacada e de fácil acesso, à Política de Privacidade ou a instrumento equivalente.

Seção III
Cláusulas-padrão Contratuais Equivalentes

Art. 18. A ANPD poderá reconhecer a equivalência de cláusulas-padrão contratuais de outros países ou de organismos internacionais com as cláusulas previstas no Anexo II.

§ 1º O procedimento para reconhecimento da equivalência de cláusulas-padrão contratuais:

I - poderá ser instaurado por decisão do Conselho Diretor, de ofício ou a requerimento dos interessados;

II - será instruído pela área técnica competente, nos termos do Regimento Interno da ANPD, que se manifestará sobre o mérito da proposta de equivalência, indicando, se for o caso, as condicionantes a serem observadas; e

III - após a manifestação da Procuradoria Federal Especializada, será objeto de deliberação pelo Conselho Diretor, na forma do Regimento Interno da ANPD.

§ 2º O Conselho Diretor poderá determinar a realização de consulta à sociedade durante o procedimento previsto no § 1º.

§3º Os órgãos e entidades da Administração Pública com competências afetas ao tema poderão ser cientificados da instauração do processo, sendo-lhes facultada a apresentação de manifestação, no âmbito de suas competências legais.

§ 4º O requerimento encaminhado à ANPD deve ser acompanhado dos seguintes documentos e informações:

I - inteiro teor das cláusulas-padrão contratuais traduzidas para o português;

II - legislação relevante aplicável e demais documentos pertinentes, incluindo guias e orientações expedidos pela respectiva autoridade de proteção de dados pessoais; e

III - análise de compatibilidade com as disposições da Lei nº 13.709, de 14 de agosto de 2018, e deste Regulamento, que inclua comparativo entre o conteúdo das cláusulas nacionais e das que se pretende obter reconhecimento de equivalência.

Art. 19. A decisão sobre a proposta de equivalência levará em consideração, entre outras circunstâncias relevantes:

I - se as cláusulas-padrão contratuais são compatíveis com as disposições da Lei nº 13.709, de

de agosto de 2018, e deste Regulamento, bem como se asseguram nível de proteção de dados equivalente ao garantido pelas cláusulas-padrão contratuais nacionais; e

II - 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 Lei nº 13.709, de 14 de agosto de 2018, além dos impactos sobre o fluxo internacional de dados, relações diplomáticas, comércio internacional e cooperação internacional do Brasil com outros países e organismos internacionais.

Parágrafo único. Para fins do disposto no inciso II do caput, a ANPD priorizará a aprovação de cláusulas que possam ser utilizadas por outros agentes de tratamento que realizam transferências internacionais de dados em circunstâncias similares.

Art. 20. As cláusulas-padrão contratuais reconhecidas como equivalentes serão aprovadas por Resolução do Conselho Diretor e publicadas na página da ANPD na Internet.

Parágrafo único. As cláusulas-padrão contratuais reconhecidas como equivalentes constituem mecanismo válido para a realização de transferências internacionais de dados, na forma do art. 33, inciso II, alínea "b", da Lei nº 13.709, de 14 de agosto de 2018, observadas as condicionantes estabelecidas na decisão do Conselho Diretor.

CAPÍTULO VI
CLÁUSULAS CONTRATUAIS ESPECÍFICAS

Art. 21. O controlador poderá solicitar à ANPD a aprovação de cláusulas contratuais específicas, que ofereçam e comprovem garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na Lei nº 13.709, de 14 de agosto de 2018, e neste Regulamento.

§ 1º As cláusulas contratuais específicas somente serão aprovadas quando a transferência internacional de dados não puder ser realizada por meio das cláusulas-padrão contratuais, em razão de circunstâncias excepcionais de fato ou de direito, devidamente comprovadas pelo controlador.

§ 2º Em qualquer hipótese, 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.

Art. 22. O controlador deverá apresentar a íntegra das cláusulas que regerão a transferência internacional de dados, incluindo as cláusulas específicas, para a aprovação pela ANPD.

§ 1º A análise efetuada pela ANPD levará em consideração, entre outras circunstâncias relevantes:

I - se as cláusulas específicas são compatíveis com as disposições da Lei nº 13.709, de 14 de agosto de 2018, e deste Regulamento, bem como se asseguram nível de proteção de dados equivalente ao garantido pelas cláusulas-padrão contratuais nacionais; e

II - 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 Lei nº 13.709, de 14 de agosto de 2018, além dos impactos quanto ao fluxo internacional de dados, relações diplomáticas, comércio internacional e cooperação internacional do Brasil com outros países e organismos internacionais.

§ 2º Para fins do disposto no inciso II do § 1º, a ANPD priorizará a aprovação de cláusulas específicas que também possam ser utilizadas por outros agentes de tratamento que realizam transferências internacionais de dados em circunstâncias similares.

Art. 23. Nas cláusulas submetidas à aprovação da ANPD, o controlador deverá:

I - adotar, sempre que possível, a redação das cláusulas-padrão contratuais; e

II - indicar as cláusulas específicas adotadas, com a respectiva justificativa, nos termos do art. 22.

Art. 24. As cláusulas contratuais específicas deverão ser submetidas à aprovação da ANPD, nos termos do processo descrito no Capítulo VIII.

CAPÍTULO VII
DAS NORMAS CORPORATIVAS GLOBAIS

Art. 25. As normas corporativas globais são destinadas às transferências internacionais de dados entre organizações do mesmo grupo ou

conglomerado de empresas, possuindo caráter vinculante em relação aos membros do grupo que as subscreverem.

Parágrafo único. A norma corporativa global constitui mecanismo válido para realizar transferências internacionais de dados pessoais apenas para as organizações ou países abrangidos pelas normas corporativas globais.

Art. 26. As normas corporativas globais deverão estar vinculadas à implementação de programa de governança em privacidade que atenda às condições mínimas estabelecidas no § 2º do art. 50 da Lei nº 13.709, de 14 de agosto de 2018.

Art. 27. Além de atender ao disposto no art. 26, as normas corporativas globais deverão conter, no mínimo:

I - descrição das 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;

II - identificação dos países para os quais os dados podem ser transferidos;

III - 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;

IV - determinação da natureza vinculante da norma corporativa global para todos os integrantes do grupo ou conglomerado de empresas que as subscreverem, inclusive para seus funcionários;

V - delimitação de responsabilidades pelo tratamento, com a indicação da entidade responsável;

VI - 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 reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;

VII - regras sobre o processo de revisão das normas corporativas globais e previsão de submissão à prévia aprovação da ANPD; e

VIII - 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 Lei nº 13.709, de 14 de agosto de 2018, especialmente na hipótese em que um dos membros do

grupo ou conglomerado de empresas estiver submetido a determinação legal de outro país que impeça o cumprimento das normas corporativas.

§ 1º Para fins de cumprimento do inciso VIII, a norma corporativa global deve prever obrigação de notificação imediata à entidade responsável sempre que um membro do grupo ou conglomerado de empresas situado em outro país esteja submetido a uma determinação legal que impeça o cumprimento das normas corporativas, ressalvada a hipótese de expressa proibição legal de realizar essa notificação.

§ 2º Para fins do inciso VI, as solicitações relacionadas ao cumprimento da norma corporativa global deverão ser respondidas no prazo previsto na Lei nº 13.709, de 14 de agosto de 2018, e em regulamentação específica.

Art. 28. As normas corporativas globais deverão ser submetidas à aprovação da ANPD, nos termos do processo descrito no Capítulo VIII.

CAPÍTULO VIII
DISPOSIÇÕES COMUNS ÀS CLÁUSULAS CONTRATUAIS ESPECÍFICAS E NORMAS CORPORATIVAS GLOBAIS

Seção I
Procedimento de Aprovação

Art. 29. O requerimento de aprovação de cláusulas contratuais específicas ou de normas corporativas globais deverá ser instruído, conforme o caso, com, no mínimo:

I - a íntegra das cláusulas ou da norma corporativa global;

II - os documentos de constituição social do agente de tratamento ou dos membros do grupo ou conglomerado de empresas;

III - se for o caso, cópia da decisão da autoridade de proteção de dados que tenha aprovado as cláusulas específicas ou normas corporativas globais objeto do requerimento de aprovação; e

IV - a demonstração do atendimento aos requisitos previstos nos Capítulos VI ou VII deste Regulamento.

Art. 30. O requerimento de aprovação de cláusulas contratuais específicas e de normas corporativas globais:

I - será analisado pela área técnica competente, nos termos do Regimento Interno da ANPD, que se manifestará sobre o mérito do pedido, indicando, se for o caso, as condicionantes a serem observadas; e

II - após a manifestação da Procuradoria Federal Especializada, será objeto de deliberação pelo Conselho Diretor, na forma do Regimento Interno da ANPD.

§ 1º Na análise das cláusulas contratuais específicas ou de normas corporativas globais submetidas à aprovação da ANPD, poderá ser requerida a apresentação de outros documentos e informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.

§ 2º O processo poderá ser arquivado, sumariamente, por decisão da área técnica competente, caso não sejam apresentados os documentos e as informações suplementares solicitados.

Seção II
Medidas de Transparência

Art. 31. A ANPD publicará em seu sítio eletrônico a relação das cláusulas contratuais específicas e das normas corporativas globais aprovadas, com indicação do respectivo requerente, da data de aprovação e da decisão proferida pelo Conselho Diretor, além de outras informações consideradas necessárias pela área técnica responsável.

Parágrafo único. A ANPD publicará a íntegra das cláusulas contratuais específicas nas hipóteses em que tais cláusulas possam ser utilizadas por outros agentes de tratamento, observados os segredos comercial e industrial.

Art. 32. O controlador deverá disponibilizar ao titular, em caso de solicitação, a íntegra das cláusulas contratuais específicas ou as normas corporativas globais, na forma prevista pelo art. 17.

Parágrafo único. O controlador publicará em sua página na Internet documento redigido em linguagem simples sobre a realização da transferência internacional de dados, na forma prevista pelo art. 17, §§ 2º e 3º, observadas as condicionantes estabelecidas na decisão de aprovação.

Seção III
Alterações

Art. 33. As alterações nas cláusulas contratuais específicas e nas normas corporativas globais dependem de prévia aprovação da ANPD, observado o procedimento descrito neste Capítulo.

Parágrafo único. O Conselho Diretor poderá estabelecer procedimento simplificado para a aprovação de alterações que não afetem as garantias apresentadas como suficientes de observância dos princípios, dos direitos do titular e do regime de proteção de dados previsto na Lei nº 13.709, de 14 de agosto de 2018.

CAPÍTULO IX
DISPOSIÇÕES FINAIS

Art. 34. Caberá pedido de reconsideração das decisões do Conselho Diretor, devidamente fundamentado, no prazo de 10 (dez) dias úteis, contados da ciência oficial pelo interessado, na forma do art. 12 do Anexo da Resolução CD/ANPD nº 1, de 28 de outubro de 2021, nos procedimentos instaurados para:

I - emissão de decisão de adequação;

II - reconhecimento de equivalência de cláusulas-padrão contratuais; ou

III - aprovação de cláusulas contratuais específicas e normas corporativas globais.

Parágrafo único. O pedido de reconsideração será distribuído e tramitará na forma do Regimento Interno da ANPD.

Anexo C – Cláusulas-Padrão Contratuais

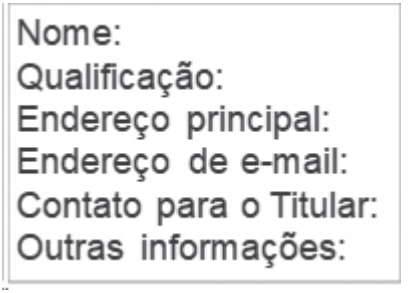
(OBS: Conforme previsto no Anexo A - Regulamento de Transferência Internacional de Dados, as Cláusulas previstas neste Anexo C poderão integrar contrato celebrado para reger, especificamente, a transferência internacional de dados ou contrato com objeto mais amplo, inclusive mediante a assinatura de termo aditivo pelo exportador e pelo importador envolvidos na operação de transferência internacional de dados).

Seção I
Informações Gerais

(OBS: Esta Seção contém Cláusulas que podem ser complementadas pelas Partes, exclusivamente, nos espaços indicados e conforme as orientações apresentadas. As definições dos termos utilizados nestas Cláusulas encontram-se detalhadas na CLÁUSULA 6).

CLÁUSULA 1. Identificação das Partes

1.1. Pelo presente instrumento contratual, o Exportador e o Importador (doravante, Partes), abaixo identificados, resolvem adotar as cláusulas-padrão contratuais (doravante Cláusulas) aprovadas pela Autoridade Nacional de Proteção de Dados (ANPD), para reger a Transferência Internacional de Dados descrita na Cláusula 2, em conformidade com as disposições da Legislação Nacional.



( ) Exportador/Controlador) ( ) Exportador/Operador)

(OBS: assinalar a opção correspondente a "Controlador" ou "Operador" e preencher com as informações de identificação, conforme indicadas no quadro).

Nome: Qualificação: Endereço principal: Endereço de e-mail: Contato para o Titular: Outras informações:

( ) Importador/Controlador ( ) Importador/Operador

(OBS: assinalar a opção correspondente a "Controlador" ou "Operador" e preencher com as informações de identificação, conforme indicadas no quadro).

CLÁUSULA 2. Objeto

2.1 Estas Cláusulas se aplicam às Transferências Internacionais de Dados do Exportador para o Importador, conforme a descrição abaixo.

Descrição da transferência internacional de dados:

Principais finalidades da transferência: Categorias de dados pessoais transferidos: Período de armazenamento dos dados: Outras informações:

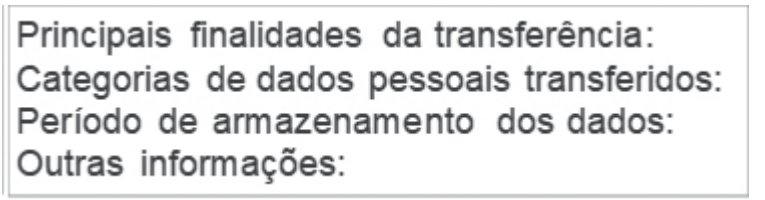
(OBS: preencher da forma mais detalhada possível com as informações relativas à transferência internacional)

CLÁUSULA 3. Transferências Posteriores

(OBS: escolher entre a "OPÇÃO A" e a "OPÇÃO B", conforme o caso.).

OPÇÃO A. 3.1. O Importador não poderá realizar Transferência Posterior dos Dados Pessoais objeto da Transferência Internacional de Dados regida por estas Cláusulas, salvo nas hipóteses previstas no item 18.3.

OPÇÃO B. 3.1. O Importador poderá realizar Transferência Posterior dos Dados Pessoais objeto da Transferência Internacional de Dados regida por estas Cláusulas nas hipóteses e conforme as condições descritas abaixo e desde que observadas as disposições da Cláusula 18.



(OBS: preencher da forma mais detalhada possível com as informações relativas às transferências posteriores autorizadas).

CLÁUSULA 4. Responsabilidades das Partes

(OBS: escolher entre a "OPÇÃO A" e a "OPÇÃO B", conforme o caso)

OPÇÃO A. (a "Opção A" é exclusiva para as transferências internacionais de dados nas quais ao menos uma das Partes atua como Controlador)

4.1 Sem prejuízo do dever de assistência mútua e das obrigações gerais das Partes, caberá à Parte Designada abaixo, na condição de Controlador, a responsabilidade pelo cumprimento das seguintes obrigações previstas nestas Cláusulas:

a) Responsável por publicar o documento previsto na Cláusula 14; ( ) Exportador ( ) Importador

b) Responsável por atender às solicitações de titulares de que trata a CLÁUSULA 15: ( ) Exportador ( ) Importador

c) Responsável por realizar a comunicação de incidente de segurança prevista na Cláusula 16: ( ) Exportador ( ) Importador

(OBS: nas alíneas "a", "b" e "c", assinalar a opção correspondente a: (i) "Exportador" ou "Importador", nos casos em que apenas uma das Partes atua como controlador; ou (ii) assinalar ambas as opções, nos casos em que as duas Partes atuam como controladores. A responsabilidade pelo cumprimento das obrigações referidas nas Cláusulas 14 a 16 não pode ser atribuída à Parte que atua como Operador. Caso se verifique, posteriormente, que a Parte Designada atua como Operador, aplicar-se-á o disposto no item 4.2)

5.1 Para os fins destas Cláusulas, verificado, posteriormente, que a Parte Designada na forma do item 4.1. atua como Operador, o Controlador permanecerá responsável:

a) pelo cumprimento das obrigações previstas nas Cláusulas 14, 15 e 16 e demais disposições estabelecidas na Legislação Nacional, especialmente em caso de omissão ou descumprimento das obrigações pela Parte Designada;

b) pelo atendimento às determinações da ANPD; e

pela garantia dos direitos dos Titulares e pela reparação dos danos causados, observado o disposto na Cláusula 17.

OPÇÃO B. (OBS: a "Opção B" é exclusiva para as transferências internacionais de dados realizadas entre operadores)

4.1 Considerando que ambas as Partes atuam, exclusivamente, como Operadores no âmbito da Transferência Internacional de Dados regida por estas Cláusulas, o Exportador declara e garante que a transferência é efetuada em conformidade com as instruções fornecidas por escrito pelo Terceiro Controlador identificado no quadro abaixo.

Informações de identificação do Terceiro Controlador:
Nome:
Qualificação:
Endereço principal:
Endereço de e-mail:
Contato para o Titular:
Informações sobre Contrato Coligado:

(OBS: preencher da forma mais detalhada possível com as informações de identificação e de contato do Terceiro Controlador e, se for o caso, do Contrato Coligado).

5.1 O Exportador responde, solidariamente, pelos danos causados pela Transferência Internacional de Dados caso está seja realizada em desconformidade com as obrigações da Legislação Nacional ou com as instruções lícitas do Terceiro Controlador, hipótese em que o Exportador se equipara a Controlador, observado o disposto na Cláusula 17.

6.1 Caso verificada a equiparação a Controlador de que trata o item 4.2, caberá ao Exportador o cumprimento das obrigações previstas nas Cláusulas 14, 15 e 16.

7.1 Ressalvado o disposto nos itens 4.2. e 4.3, não se aplica às Partes, na condição de Operadores, o disposto nas Cláusulas 14, 15 e 16.

8.1 As Partes fornecerão, em qualquer hipótese, todas as informações de que dispuserem e que se demonstrarem necessárias para que o Terceiro Controlador possa atender a determinações da ANPD e cumprir adequadamente obrigações previstas na Legislação Nacional relacionadas à transparência, ao atendimento a direitos dos titulares e à comunicação de incidentes de segurança à ANPD.

9.1 As Partes devem promover assistência mútua com a finalidade de atender às solicitações dos Titulares.

10.1 Em caso de recebimento de solicitação de Titular, a Parte deverá:

a) atender à solicitação, quando dispuser das informações necessárias;

b) informar ao Titular o canal de atendimento disponibilizado pelo Terceiro Controlador; ou

c) encaminhar a solicitação para o Terceiro Controlador o quanto antes, a fim de viabilizar a resposta no prazo previsto na Legislação Nacional.

11.1 As Partes devem manter o registro de incidentes de segurança com dados pessoais, nos termos da Legislação Nacional.

Seção II
Cláusulas Mandatórias

(OBS: Esta Seção contém Cláusulas que devem ser adotadas integralmente e sem qualquer alteração em seu texto a fim de assegurar a validade da transferência internacional de dados).

CLÁUSULA 5. Finalidade

Estas Cláusulas se apresentam como mecanismo viabilizador do fluxo internacional seguro de dados pessoais, estabelecem garantias mínimas e condições válidas para a realização de Transferência Internacional de Dados e visam garantir a adoção das salvaguardas adequadas para o cumprimento dos princípios, dos direitos do Titular e do regime de proteção de dados previstos na Legislação Nacional.

CLÁUSULA 6. Definições

6.1 Para os fins destas Cláusulas, serão consideradas as definições do art. 5º da Lei nº 13.709, de 14 de agosto de 2018, e do art. 3º do Regulamento de Transferência Internacional de Dados Pessoais, sem prejuízo de outros atos normativos expedidos pela ANPD. As Partes concordam, ainda, em considerar os termos e seus respectivos significados, conforme exposto a seguir:

a) Agentes de tratamento: o controlador e o operador;

b) ANPD: Autoridade Nacional de Proteção de Dados;

c) Cláusulas: as cláusulas-padrão contratuais aprovadas pela ANPD, que integram as Seções I, II e III;

d) Contrato Coligado: instrumento contratual firmado entre as Partes ou, pelo menos, entre uma destas e um terceiro, incluindo um Terceiro Controlador, que possua propósito comum, vinculação ou relação de dependência com o contrato que rege a Transferência Internacional de Dados;

e) Controlador: Parte ou terceiro ("Terceiro Controlador") a quem compete as decisões referentes ao tratamento de Dados Pessoais;

f) Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável;

g) Dado Pessoal Sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

h) Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

i) Exportador: agente de tratamento, localizado no território nacional ou em país estrangeiro, que transfere dados pessoais para Importador;

j) Importador: agente de tratamento, localizado em país estrangeiro ou que seja organismo internacional, que recebe dados pessoais transferidos por Exportador;

k) Legislação Nacional: conjunto de dispositivos constitucionais, legais e regulamentares brasileiros a respeito da proteção de Dados Pessoais, incluindo a Lei nº 13.709, de 14 de agosto de 2018, o Regulamento de Transferência Internacional de Dados e outros atos normativos expedidos pela ANPD;

l) Lei de Arbitragem: Lei nº 9.307, de 23 de setembro de 1996;

m) Medidas de Segurança: medidas técnicas e administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

n) Órgão de Pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

o) Operador: Parte ou terceiro, incluindo um Subcontratado, que realiza o tratamento de Dados Pessoais em nome do Controlador;

p) Parte Designada: Parte do contrato designada, nos termos da Cláusula 4 ("Opção A"), para cumprir, na condição de Controlador, obrigações específicas relativas à transparência, direitos dos Titulares e comunicação de incidentes de segurança;

q) Partes: Exportador e Importador;

t) Solicitação de Acesso: solicitação de atendimento obrigatório, por força de lei, regulamento ou determinação de autoridade pública, para conceder acesso aos Dados Pessoais objeto da Transferência Internacional de Dados regida por estas Cláusulas;

s) Subcontratado: agente de tratamento contratado pelo Importador, sem vínculo com o Exportador, para realizar tratamento de Dados Pessoais após uma Transferência Internacional de Dados;

t) Terceiro Controlador: Controlador dos Dados Pessoais que fornece instruções por escrito para a realização, em seu nome, da Transferência Internacional de Dados entre Operadores regida por estas Cláusulas, na forma da Cláusula 4 ("Opção B");

u) Titular: pessoa natural a quem se referem os Dados Pessoais que são objeto da Transferência Internacional de Dados regida por estas Cláusulas;

v) Transferência: modalidade de tratamento por meio da qual um agente de tratamento transmite, compartilha ou disponibiliza acesso a Dados Pessoais a outro agente de tratamento;

w) Transferência Internacional de Dados: transferência de Dados Pessoais para país estrangeiro ou organismo internacional do qual o país seja membro; e

x) Transferência Posterior: transferência Internacional de Dados, originada de um Importador, e destinada a um terceiro, incluindo um Subcontratado, desde que não configure Solicitação de Acesso.

CLÁUSULA 7. Legislação aplicável e fiscalização da ANPD

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

CLÁUSULA 8. Interpretação

8.1. Qualquer aplicação destas Cláusulas deve ocorrer de acordo com os seguintes termos:

a) estas Cláusulas devem sempre ser interpretadas de forma mais favorável ao Titular e de acordo com as disposições da Legislação Nacional;

b) em caso de dúvida sobre o significado de termos destas Cláusulas, aplica-se o significado que mais se alinha com a Legislação Nacional;

c) nenhum item destas Cláusulas, incluindo-se aqui um Contrato Coligado e as disposições previstas na Seção IV, poderá ser interpretado com o objetivo de limitar ou excluir a responsabilidade de qualquer uma das Partes em relação a obrigações previstas na Legislação Nacional; e

d) as disposições das Seções I e II prevalecem em caso de conflito de interpretação com Cláusulas adicionais e demais disposições previstas nas Seções III e IV deste instrumento ou em Contratos Coligados.

CLÁUSULA 9. Possibilidade de adesão de terceiros

9.1. Em comum acordo entre as Partes, é possível a um agente de tratamento aderir a estas Cláusulas na condição de Exportador ou de Importador, por meio do preenchimento e assinatura de documento escrito, que integrará o presente instrumento.

1.2. A parte aderente terá os mesmos direitos e obrigações das Partes originárias, conforme a posição assumida de Exportador ou Importador e de acordo com a categoria de agente de tratamento correspondente.

CLÁUSULA 10. Obrigações gerais das Partes

10.1. As Partes se comprometem a adotar e, quando necessário, demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das disposições destas Cláusulas e da Legislação Nacional e, inclusive, da eficácia dessas medidas e, em especial:

a) utilizar os Dados Pessoais somente para as finalidades específicas descritas na Cláusula 2, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades, observadas, em qualquer caso, as limitações, garantias e salvaguardas previstas nestas Cláusulas;

b) garantir a compatibilidade do tratamento com as finalidades informadas ao Titular, de acordo com o contexto do tratamento;

c) limitar o tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de Dados Pessoais;

d) garantir aos Titulares, observado o disposto na Cláusula 4.

(d.1.) informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

(d.2.) consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus Dados Pessoais; e

(d.3.) a exatidão, clareza, relevância e atualização dos Dados Pessoais, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

e) adotar as medidas de segurança apropriadas e compatíveis com os riscos envolvidos na Transferência Internacional de Dados regida por estas Cláusulas;

f) não realizar tratamento de Dados Pessoais para fins discriminatórios ilícitos ou abusivos;

g) assegurar que qualquer pessoa que atue sob sua autoridade, inclusive subcontratados ou qualquer agente que com ele colabore, de forma gratuita ou onerosa, realize tratamento de dados apenas em conformidade com suas instruções e com o disposto nestas Cláusulas; e

h) manter registro das operações de tratamento dos Dados Pessoais objeto da Transferência Internacional de Dados regida por estas Cláusulas, e apresentar a documentação pertinente à ANPD, quando solicitado.

CLÁUSULA 11. Dados pessoais sensíveis

11.1. Caso a Transferência Internacional de Dados envolva Dados Pessoais sensíveis, as Partes aplicarão salvaguardas adicionais, incluindo medidas de segurança específicas e proporcionais aos riscos da atividade de tratamento, à natureza específica dos dados e aos interesses, direitos e garantias a serem protegidos, conforme descrito na Seção III.

CLÁUSULA 12. Dados pessoais de crianças e adolescentes

12.1. Caso a Transferência Internacional de Dados envolva Dados Pessoais de crianças e adolescentes, as Partes aplicarão salvaguardas adicionais, incluindo medidas que assegurem que o tratamento seja realizado em seu melhor interesse, nos termos da Legislação Nacional e dos instrumentos pertinentes de direito internacional.

CLÁUSULA 13. Uso legal dos dados

13.1. O Exportador garante que os Dados Pessoais foram coletados, tratados e transferidos para o Importador de acordo com a Legislação Nacional.

CLÁUSULA 14. Transparência

1.1. A Parte Designada publicará, em sua página na Internet, documento contendo informações facilmente acessíveis redigidas em linguagem simples, clara e precisa sobre a realização da Transferência Internacional de Dados, incluindo, pelo menos, informações sobre:

a) a forma, a duração e a finalidade específica da transferência internacional;

b) o país de destino dos dados transferidos;

c) a identificação e os contatos da Parte Designada;

d) o uso compartilhado de dados pelas Partes e a finalidade;

e) as responsabilidades dos agentes que realizarão o tratamento;

f) os direitos do Titular e os meios para o seu exercício, incluindo canal de fácil acesso disponibilizado para atendimento às suas solicitações e o direito de peticionar contra o Controlador perante a ANPD; e

g) Transferências Posteriores, incluindo as relativas aos destinatários e à finalidade da transferência.

2.1. O documento referido no item 14.1. poderá ser disponibilizado em página específica ou integrado, de forma destacada e de fácil acesso, à Política de Privacidade ou documento equivalente.

3.1. A pedido, as Partes devem disponibilizar, gratuitamente, ao Titular uma cópia destas Cláusulas, observados os segredos comercial e industrial.

4.1. Todas as informações disponibilizadas aos titulares, nos termos destas Cláusulas, deverão ser redigidas na língua portuguesa.

CLÁUSULA 15. Direitos do Titular

15.1. O Titular tem direito a obter da Parte Designada, em relação aos Dados Pessoais objeto da Transferência Internacional de Dados regida por estas Cláusulas, a qualquer momento, e mediante requisição, nos termos da Legislação Nacional:

a) confirmação da existência de tratamento;

b) acesso aos dados;

c) correção de dados incompletos, inexatos ou desatualizados;

d) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com estas Cláusulas e com o disposto na Legislação Nacional;

e) portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da ANPD, observados os segredos comercial e industrial;

f) eliminação dos Dados Pessoais tratados com o consentimento do Titular, exceto nas hipóteses previstas na Cláusula 20;

g) informação das entidades públicas e privadas com as quais as Partes realizaram uso compartilhado de dados;

h) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

i) revogação do consentimento mediante procedimento gratuito e facilitado, ratificados os tratamentos realizados antes do requerimento de eliminação;

j) revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as

decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade; e

k) informações a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

16.1. O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nestas Cláusulas ou na Legislação Nacional.

17.1. O prazo para atendimento às solicitações previstas nesta Cláusula e no item 14.3. é de 15 (quinze) dias contados da data do requerimento do titular, ressalvada a hipótese de prazo distinto estabelecido em regulamentação específica da ANPD.

18.1. Caso a solicitação do Titular seja direcionada à Parte não designada como responsável pelas obrigações previstas nesta Cláusula ou no item 14.3., a Parte deverá:

a) informar ao Titular o canal de atendimento disponibilizado pela Parte Designada; ou

b) encaminhar a solicitação para a Parte Designada o quanto antes, a fim de viabilizar a resposta no prazo previsto no item 15.2.

19.1. As Partes deverão informar, imediatamente, aos Agentes de Tratamento com os quais tenham realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.

20.1. As Partes devem promover assistência mútua com a finalidade de atender às solicitações dos Titulares.

CLÁUSULA 16. Comunicação de Incidente de Segurança

16.1. A Parte Designada deverá comunicar à ANPD e aos Titulares, no prazo de 3 (três) dias úteis, a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante para os Titulares, observado o disposto na Legislação Nacional.

17.1. O Importador deve manter o registro de incidentes de segurança nos termos da Legislação Nacional

CLÁUSULA 17. Responsabilidade e ressarcimento de danos

17.1 A Parte que, em razão do exercício da atividade de tratamento de Dados Pessoais, causar dano patrimonial, moral, individual ou coletivo, em violação às disposições destas Cláusulas e da Legislação Nacional, é obrigada a repará-lo.

1º.1 O Titular poderá pleitear a reparação do dano causado por quaisquer das Partes em razão da violação destas Cláusulas.

19.1 A defesa dos interesses e dos direitos dos Titulares poderá ser pleiteada em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente acerca dos instrumentos de tutela individual e coletiva.

20.1 A Parte que atuar como Operador responde, solidariamente, pelos danos causados pelo tratamento quando descumprir as presentes Cláusulas ou quando não tiver seguido as instruções lícitas do Controlador, ressalvado o disposto no item 17.6.

21.1 Os Controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao Titular respondem, solidariamente, por estes danos, ressalvado o disposto no item 17.6.

22.1 Não caberá responsabilização das Partes se comprovado que:

a) não realizaram o tratamento de Dados Pessoais que lhes é atribuído;

b) embora tenham realizado o tratamento de Dados Pessoais que lhes é atribuído, não houve violação a estas Cláusulas ou à Legislação Nacional; ou

c) o dano é decorrente de culpa exclusiva do Titular ou de terceiro que não seja destinatário de Transferência Posterior ou subcontratado pelas Partes.

23.1. Nos termos da Legislação Nacional, o juiz poderá inverter o ônus da prova a favor do Titular quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo Titular resultar-lhe excessivamente onerosa.

24.1. As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos desta Cláusula podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

25.1 A Parte que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

CLÁUSULA 18. Salvaguardas para Transferência Posterior

18.1 O Importador somente poderá realizar Transferências Posteriores dos Dados Pessoais objeto da Transferência Internacional de Dados regida por estas Cláusulas se expressamente autorizado, conforme as hipóteses e condições descritas na Cláusula 3.

19.1 Em qualquer caso, o Importador:

a) deve assegurar que a finalidade da Transferência Posterior é compatível com as finalidades específicas descritas na Cláusula 2;

b) deve garantir, mediante instrumento contratual escrito, que as salvaguardas previstas nestas Cláusulas serão observadas pelo terceiro destinatário da Transferência Posterior; e

c) para fins destas Cláusulas, e em relação aos Dados Pessoais transferidos, será considerado o responsável por eventuais irregularidades praticadas pelo terceiro destinatário da Transferência Posterior.

20.1. A Transferência Posterior poderá, ainda, ser realizada com base em outro mecanismo válido de Transferência Internacional de Dados previsto na Legislação Nacional, independentemente da autorização de que trata a Cláusula 3.

CLÁUSULA 19. Notificação de Solicitação de Acesso

19.1. O Importador notificará o Exportador e o Titular sobre Solicitação de Acesso relacionada aos Dados Pessoais objeto da Transferência Internacional de Dados regida por estas Cláusulas, ressalvada a hipótese de vedação de notificação pela lei do país de tratamento dos dados.

20.1. O Importador adotará as medidas legais cabíveis, incluindo ações judiciais, para proteger os direitos dos Titulares sempre que houver fundamento jurídico adequado para questionar a legalidade da Solicitação de Acesso e, se for o caso, a vedação de realizar a notificação referida no item 19.1.

21.1. Para atender às solicitações da ANPD e do Exportador, o Importador deve manter registro de Solicitações de Acesso, incluindo data, solicitante, finalidade da solicitação, tipo de dados solicitados, número de solicitações recebidas e medidas legais adotadas.

CLÁUSULA 20. Término do tratamento e eliminação dos dados

20.1. As Partes deverão eliminar os Dados Pessoais objeto da Transferência Internacional de Dados regida por estas Cláusulas após o término do tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação apenas para as seguintes finalidades:

a) cumprimento de obrigação legal ou regulatória pelo Controlador;

b) estudo por Órgão de Pesquisa, garantida, sempre que possível, a anonimização dos Dados Pessoais;

c) transferência a terceiro, desde que respeitados os requisitos previstos nestas Cláusulas e na Legislação Nacional; e

d) uso exclusivo do Controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

21.1. Para fins desta Cláusula, considera-se que o término do tratamento ocorrerá quando:

a) alcançada a finalidade prevista nestas Cláusulas;

b) os Dados Pessoais deixarem de ser necessários ou pertinentes ao alcance da finalidade específica prevista nestas Cláusulas;

c) finalizado o período de tratamento;

d) atendida solicitação do Titular; e

e) determinado pela ANPD, quando houver violação ao disposto nestas Cláusulas ou na Legislação Nacional.

CLÁUSULA 21. Segurança no tratamento dos dados

21.1. As Partes deverão adotar medidas de segurança que garantam proteção aos Dados Pessoais objeto da Transferência Internacional de Dados regida por estas Cláusulas, mesmo após o seu término.

22.1. As Partes informarão, na Seção III, as Medidas de Segurança adotadas, considerando a natureza das informações tratadas, as características específicas e a finalidade do tratamento, o estado atual da tecnologia e os riscos para os direitos dos Titulares, especialmente no caso de dados pessoais sensíveis e de crianças e adolescentes.

23.1. As Partes deverão realizar os esforços necessários para adotar medidas periódicas de avaliação e revisão visando manter nível de segurança adequado às características do tratamento de dados.

CLÁUSULA 22. Legislação do país destinatário dos dados

22.1. O Importador declara que não identificou leis ou práticas administrativas do país destinatário dos Dados Pessoais que o impeçam de cumprir as obrigações assumidas nestas Cláusulas.

23.1. Sobrevindo alteração normativa que altere esta situação, o Importador notificará, de imediato, o Exportador para avaliação da continuidade do contrato.

CLÁUSULA 23. Descumprimento das Cláusulas pelo Importador

23.1. Havendo violação das salvaguardas e garantias previstas nestas Cláusulas ou a impossibilidade de seu cumprimento pelo Importador, o Exportador deverá ser comunicado imediatamente, ressalvado o disposto no item 19.1.

24.1. Recebida a comunicação de que trata o item 23.1 ou verificado o descumprimento destas Cláusulas pelo Importador, o Exportador adotará as providências pertinentes para assegurar a proteção aos direitos dos Titulares e a conformidade da Transferência Internacional de Dados com a Legislação Nacional e as presentes Cláusulas, podendo, conforme o caso:

a) suspender a Transferência Internacional de Dados;

b) solicitar a devolução dos Dados Pessoais, sua transferência a um terceiro, ou a sua eliminação; e

c) rescindir o contrato.

CLÁUSULA 24. Eleição do foro e jurisdição

24.1. Aplica-se a estas Cláusulas a legislação brasileira e qualquer controvérsia entre as Partes decorrente destas Cláusulas será resolvida perante os tribunais competentes do Brasil, observado, se for o caso, o foro eleito pelas Partes na Seção IV.

25.1. Os Titulares podem ajuizar ações judiciais contra o Exportador ou o Importador, conforme sua escolha, perante os tribunais competentes no Brasil, inclusive naqueles localizados no local de sua residência.

26.1. Em comum acordo, as Partes poderão se valer da arbitragem para resolver os conflitos decorrentes destas Cláusulas, desde que realizada no Brasil e conforme as disposições da Lei de Arbitragem.

Seção III
Medidas De Segurança

(OBS: Nesta Seção deve ser incluído o detalhamento das medidas de segurança adotadas, incluindo medidas específicas para a proteção de dados sensíveis e de crianças e adolescentes. As medidas podem contemplar, entre outros, os seguintes aspectos, conforme indicados no quadro abaixo).

(i) governança e supervisão de processos internos; (ii) medidas de segurança técnicas e administrativas, incluindo medidas para garantir a segurança das operações realizadas, tais como a coleta, a transmissão e o armazenamento dos dados;

Seção IV
Cláusulas Adicionais e Anexos

(OBS: Nesta Seção, de preenchimento e de divulgação facultativos, podem ser incluídas Cláusulas Adicionais e Anexos, a critério das Partes, para disciplinar, entre outras, questões de natureza comercial, rescisão contratual, prazo de vigência e eleição de foro no Brasil. Conforme previsto no Regulamento de Transferência Internacional de Dados, as Cláusulas estabelecidas nesta Seção ou em Contratos Coligados não poderão excluir, modificar ou contrariar, direta ou indiretamente, as Cláusulas previstas nas Seções I, II e III).

Local, data. Assinaturas.

Capítulo 2
As Cláusulas-Padrão Contratuais para Transferência Internacional da Rede Ibero-Americana de Proteção de Dados (RIPD) como Forma de Harmonização Latino-Americana

Introdução

No capítulo anterior, examinamos as regras existentes em cada um dos países analisados sobre a transferência internacional de dados pessoais e algumas ferramentas para proteger o fluxo de dados dentro da região latino-americana. Emerge do capítulo anterior que na região existem diferentes regulações com um histórico comum, mas com falta de harmonização nas ferramentas a serem utilizadas para simplificar a transferência internacional de dados pessoais.

Neste capítulo, examinamos as Cláusulas-padrão contratuais (SCCs) desenvolvidas pela Rede Ibero-Americana de Proteção de Dados Pessoais, uma vez que são as ferramentas mais utilizadas para a transferência internacional entre empresas e um dos caminhos para alcançar um efeito harmonizador na região latino-americana.

1 A Rede Ibero-Americana de Proteção de Dados

1.1 Origem da rede

A Rede Ibero-Americana de Proteção de Dados (RIPD) foi criada como resultado do acordo alcançado no Encontro Ibero-Americano de Proteção de Dados (EIPD) realizado em La Antigua (Guatemala) em junho de

2003, com a presença de representantes de 14 países ibero-americanos. Desde o início, esta iniciativa contou com apoio político, refletido na Declaração Final da XIII Cúpula de Chefes de Estado e de Governo dos Países Ibero-Americanos, realizada em Santa Cruz de la Sierra, Bolívia, em 14 e 15 de novembro de 2003, consciente da natureza da proteção de dados pessoais como um direito fundamental, bem como da importância das iniciativas regulatórias ibero-americanas para proteger a privacidade dos cidadãos.

A RIPD configurou-se assim desde suas origens como um fórum integrador para os diversos atores, tanto do setor público quanto do privado e da academia, que desenvolvem iniciativas e projetos relacionados à proteção de dados pessoais na Ibero-América, a fim de promover, manter e fortalecer um intercâmbio próximo e permanente de informações, experiências e conhecimentos entre eles, bem como promover os desenvolvimentos normativos necessários para garantir uma regulação avançada do direito à proteção de dados pessoais em um contexto democrático, levando em consideração a necessidade do fluxo contínuo de dados entre países que possuem diversos laços em comum e uma preocupação com esse direito.

1.2 Normas ibero-americanas

O marco no trabalho da RIPD, do ponto de vista regulatório, deve ser encontrado, sem dúvida, na aprovação em junho de 2017, no âmbito do XV Encontro Ibero-Americano em Santiago do Chile, das "Normas de Proteção de Dados Pessoais para Estados Ibero-americanos", que contaram com o apoio da própria Comissão Europeia e foram um passo importante para a regulação da proteção de dados na região.

As Normas buscam ser o modelo de referência para a futura regulação da lei de proteção de dados na região, bem como para a revisão das normas existentes para sua atualização de acordo com seus parâmetros. Isso é expresso em sua parte introdutória, quando afirma que

> as Normas Ibero-Americanas constituem um conjunto de diretrizes orientadoras que contribuem para a emissão de iniciativas regulatórias para a proteção de dados pessoais na região ibero-americana daqueles países que ainda não possuem essas normas, ou, se for o caso, servem de referência para a modernização e atualização da legislação existente.

Especificamente, com a aprovação das Normas, pretende-se os seguintes objetivos:

(i) Estabelecer um conjunto de princípios e direitos comuns para a proteção de dados pessoais que os Estados ibero-americanos possam adotar e desenvolver em sua legislação nacional, a fim de ter regras homogêneas na região.

(ii) Garantir o exercício efetivo e a proteção do direito à proteção de dados pessoais de qualquer pessoa física nos Estados ibero-americanos, por meio do estabelecimento de regras comuns que assegurem o tratamento adequado de seus dados pessoais.

(iii) Facilitar o fluxo de dados pessoais entre os Estados ibero-americanos e além de suas fronteiras, a fim de contribuir para o crescimento econômico e social da região.

(iv) Promover a cooperação internacional entre as autoridades de supervisão dos Estados ibero-americanos, com outras autoridades de supervisão não pertencentes à região e autoridades e organizações internacionais na matéria.

Em 2017, os membros do RIPD aprovaram as Normas de Proteção de Dados Pessoais para os Estados Ibero-americanos. Estas Normas buscam estabelecer um conjunto de princípios e direitos comuns para a proteção de dados pessoais que os Estados ibero-americanos podem adotar e desenvolver em sua legislação nacional, a fim de ter regras homogêneas na região. Por outro lado, as Normas Ibero-Americanas incluem as melhores práticas nacionais e internacionais na área no momento de sua emissão.

Entre os objetivos das Normas Ibero-Americanas estão os seguintes, que de alguma forma justificam a adoção de SCCs para a região:

(i) facilitar o fluxo de dados pessoais entre os Estados ibero-americanos e além de suas fronteiras, a fim de contribuir para o crescimento econômico e social da região; e

(ii) promover a cooperação internacional entre as autoridades de supervisão dos Estados ibero-americanos, com outras autoridades de supervisão não pertencentes à região e autoridades e organizações internacionais na matéria.

O nº 1, alínea c), do artigo 36º das normas estabelece que

> O controlador e o processador podem realizar transferências internacionais de dados pessoais em qualquer um dos seguintes casos:
> (…)
> c. O exportador e o destinatário assinam cláusulas contratuais ou qualquer outro instrumento legal que ofereça garantias suficientes e que permita demonstrar o alcance do tratamento de dados pessoais, as obrigações e responsabilidades assumidas pelas partes e os direitos dos titulares. A autoridade supervisora pode validar cláusulas contratuais ou instrumentos legais conforme determinado na legislação nacional dos Estados ibero-americanos aplicável na matéria.

Das Normas Ibero-Americanas emerge o seguinte:

- O Exportador e o Importador podem celebrar cláusulas contratuais.
- Estas cláusulas contratuais devem oferecer garantias suficientes, que permitam demonstrar: (i) o âmbito do tratamento de dados pessoais, (ii) as obrigações e responsabilidades assumidas pelas partes e (iii) os direitos dos Titulares dos Dados.
- A respectiva autoridade supervisora poderá validar cláusulas contratuais ou instrumentos jurídicos conforme determinado na legislação nacional dos Estados ibero-americanos aplicável na matéria.

Por fim, na reunião da RIPD realizada em Cartagena (Colômbia) de 27 a 29 de maio de 2024, foram apresentadas as bases para atualização dos padrões de Rede aprovados em 2017. Em particular, este trabalho visa modernizar as Normas para:

- Promover o fortalecimento do tratamento adequado de dados pessoais e a proteção dos direitos das pessoas no âmbito das tecnologias emergentes (como neurotecnologias e inteligência artificial), bem como seu uso ético e responsável.
- Reforçar a proteção dos menores em ambientes digitais no que diz respeito ao tratamento dos seus dados pessoais.

- Garantir que as autoridades de proteção de dados tenham mais recursos, autonomia e independência para poderem cumprir devida e atempadamente as suas funções.

1.3 Outros documentos da RIPD

Nos últimos anos, a Rede emitiu vários documentos relevantes[84] para alimentar o debate regional sobre transferências de dados, incluindo os seguintes:

- Recomendações Gerais para Tratamento de Dados em Inteligência Artificial;
- Recomendações para o tratamento de dados pessoais utilizando serviços de computação em nuvem;
- Recomendações do RIPD para o tratamento de dados pessoais de saúde em tempos de pandemia;
- Modelo de cláusulas contratuais para a região, que analisaremos no próximo ponto.

2 Cláusulas-padrão contratuais

2.1 Conceito

As cláusulas-padrão contratuais (SCCs) são cláusulas contratuais modelo "pré-aprovadas" por um regulador de proteção de dados pessoais que são estabelecidas para garantir a transferência internacional de dados, observando o cumprimento das diferentes medidas de proteção estabelecidas em relação ao tratamento de dados pessoais.

A UE tem uma longa história de utilização de cláusulas contratuais. Vários modelos foram projetados sob a Diretiva de Proteção de Dados de 1995.[85]

---

84 Os documentos podem ser consultados neste site: RIPD. Guias/Orientações. RIPD. 2023. Disponível em: https://www.redipd.org/es/documentos/guias.

85 Consulte PALAZZI. *Contratos de Tratamento de Dados. Coordenação, redação e negociação* (Justin Weiss, ed.), IAPP, Capítulo sobre contratos de transferência internacional de dados pessoais. New Hampshire: IAPP, 2023.

Sob a vigência do GDPR, a Comissão Europeia aprovou em junho de 2021 um novo conjunto de cláusulas contratuais a serem usadas por quem transfere dados para fora da Europa. A aprovação dessas cláusulas-padrão motivou a RIPD a se interessar em gerar um modelo semelhante para a América Latina.

2.2 Vantagens das cláusulas-padrão contratuais para a América Latina

O uso de Cláusulas-padrão contratuais (SCCs) pode ajudar a superar possíveis limitações nas transferências de dados resultantes de diferenças no nível de proteção entre diferentes países.

A instituição do contrato e o conceito de terceiros beneficiários estão presentes em todos os ordenamentos jurídicos Ibero-Americanos e servem para obrigar o "importador de dados" a respeitar os dados pessoais do titular, uma vez que os dados pessoais estejam na jurisdição de destino e a dar direitos ao titular em outra jurisdição, apesar de não fazer parte dela.

Em outras palavras: cláusulas-padrão ou cláusulas tipo contribuem para construir convergência a nível contratual, criando um regime autônomo de proteção de dados, sem necessariamente exigir convergência a nível de país (nisso, podem ir além do nível de proteção em determinados países).

Ao mesmo tempo, a expansão dos princípios de proteção de dados pessoais por meio de redes contratuais internacionais tem um forte impacto na convergência geral da região, pois estabelecem padrões comuns com os quais as empresas se familiarizam. Isso facilitará no futuro o alinhamento da legislação nacional com as normas e padrões internacionais de proteção de dados pessoais.

Por outro lado, a utilização das SCCs serve para garantir os princípios e deveres na proteção de dados pessoais. Isto, por sua vez, conduz à transparência, à segurança jurídica e, por conseguinte, à previsibilidade, uma vez que:

i) através do seu caráter vinculante e executório no âmbito de um contrato, podem assegurar a continuidade da proteção quando os dados viajam para o estrangeiro, e fazê-lo de uma forma que proporcione segurança jurídica;

ii) ao fazê-lo de forma clara e transparente, contribuem para a criação de confiança, o que, por sua vez, confere às empresas que utilizam tais cláusulas uma vantagem competitiva em relação às que têm de recorrer a outros métodos.

As SCCs servem para proteger a parte "mais fraca", que obviamente são as pessoas físicas cujos dados pessoais, no âmbito das transferências internacionais de dados pessoais (TIDP), são tratados tanto pelo Exportador de Dados quanto pelo Importador de Dados.

Por último, a utilização de SCCs permite também uma solução particularmente eficaz em termos de custos para o problema do TID; a razão para tal é que as empresas não têm de negociar acordos numa base casuística com o custo econômico que isso implica em termos de representação legal e de tempo. A existência das SCCs permite que eles contem com o modelo pré-aprovado pela Autoridade de Supervisão competente, sabendo que ao fazê-lo cumprem com suas obrigações legais relativas à transferência internacional de dados pessoais com uma solução simples e prática. Essa é uma grande diferença em relação a outras ferramentas, como mecanismos de certificação ou Regras Corporativas Vinculantes (BCRs), que exigem um processo de certificação muitas vezes demorado e caro. Em comparação com esses mecanismos, as SCCs são um instrumento "pronto para uso" e "pronto para execução". Isso é particularmente importante para pequenas e médias empresas que não podem pagar outras opções mais caras que exigem mais tempo para serem implementadas. É por isso que as SCCs são o mecanismo legal mais acessível e amplamente utilizado para a TIDP para jurisdições inadequadas. Estima-se que cerca de 80 a 90% das empresas que implementam mecanismos de TIDP utilizam os SCCs como solução.

Obviamente, isso implica que as Partes de um TIDP utilizam uma SSC não devem se limitar ao requisito formal de sua assinatura, mas devem estar sempre preparadas para "prestar contas" pelo tratamento de dados pessoais à Autoridade Supervisora competente e aos Titulares dos Dados e ser capazes de demonstrar total conformidade com a lei aplicável e as obrigações impostas nas SCCs.

2.3 O sistema europeu de cláusulas-modelo

A União Europeia (UE), por meio do Regulamento Geral de Proteção de Dados (GDPR), estabelece quatro módulos de SCCs, para os contratos internacionais de transferência de dados celebrados entre controladores e operadores de dados localizados em um país membro da UE

que desejam transferir dados pessoais para outro controlador ou para um localizado em um país não membro.

Os módulos contêm cláusulas em função dos diferentes tipos de contratos que podem ser celebrados. Nesse sentido, o módulo um se concentra nas transferências de controlador para controlador, o módulo dois nas transferências de controlador para operador, o módulo três nas transferências de operador para operador e o módulo quatro nas transferências de operador para controlador.

A razão pela qual estas cláusulas pré-estabelecidas são criadas é para garantir que, no país de destino (não membro da UE), os dados estejam devidamente protegidos, salvaguardando o direito dos titulares dos dados, garantido pelo GDPR, a terem os seus dados armazenados com a devida segurança para evitar a sua fuga ou divulgação ilegítima.

Quando o contrato for celebrado por duas partes sediadas em países membros da UE, não será obrigatória a inclusão das SCCs, uma vez que ambas devem cumprir previamente os requisitos de segurança e privacidade estabelecidos pelo GDPR.

2.4 As cláusulas-padrão contratuais para a transferência internacional de dados pessoais da Rede Ibero-Americana de Proteção de Dados

A RIPD, durante a presidência da Colômbia, decidiu adotar cláusulas-padrão para a região, visto que naquela época poucos países (apenas Argentina e Uruguai) tinham cláusulas-padrão ou "diretrizes" para elaborar esse tipo de contrato.

Felizmente, a RIPD conta com a presença da Espanha (a AEPD é responsável pelo secretariado permanente) e Portugal, que, sendo membros da UE, participaram em duas décadas de experiência da comunidade europeia na matéria. Assim, com o apoio da Comissão Europeia, avançou-se com a elaboração de dois modelos de contratos e um guia explicativo, que são anexos a este trabalho.

Após um período de recebimento de comentários e aprovação de uma versão final, em 27 de setembro de 2022, a Secretaria Permanente da RIPD publicou em seu site o Guia para a Implementação de Cláusulas Contra-

tuais Modelo para a Transferência Internacional de Dados Pessoais e seus Anexos, a fim de estabelecer os principais aspectos a serem levados em consideração quando as transferências internacionais de dados pessoais são feitas por meio do uso de Cláusulas-padrão contratuais.[86]

2.5 Adoção pelos países latino-americanos

Em 2021, Argentina e Uruguai foram os únicos países que tiveram cláusulas-padrão contratuais reguladas. Na ausência de normas vigentes na região, a RIPD decidiu empreender o projeto de um modelo de cláusulas contratuais juntamente com um Guia para sua implementação.

Como dissemos anteriormente, os países da região podem adotar essas cláusulas-padrão de várias maneiras: *i)* Uma é declarar obrigatoriamente que as cláusulas-padrão contratuais são a forma de implementar uma solução contratual; *ii)* Outra é simplesmente recomendá-los como uma opção possível dentro da liberdade contratual que as partes têm; e *iii)* Também seria possível dar vários modelos como alternativas, como opções dentro das formas possíveis de fazer transferências seguras.

Além disso, as agências de proteção de dados dos diversos países latino-americanos podem adicionar outras precauções, como, por exemplo, a realização de uma *due diligence* sobre a adequação do país de destino ou medidas adicionais, conforme sugerido pelo EDPB após o caso "Schrems II".

2.5.1 Peru

Em 17 de outubro de 2022, por meio da Resolução da Diretoria nº 0074-2022-JUS/DGTAIPD, a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) do Ministério da Justiça e Direitos Humanos (MinJus-DH) do Peru aprovou as Cláusulas-padrão contratuais (SCC) da RIPD para a transferência internacional de dados pessoais.[87]

86 Rede Ibero-Americana de Proteção de Dados, Modelos de cláusulas contratuais. RIPD. 2023. Disponível em: https://www.redipd.org/es/documentos/guias.

87 BRIAN, Ana. Cláusulas Contratuais Modelo para a Transferência Internacional de Dados Pessoais: O Caso do Peru, *A Lei de Privacidade*, n. 14, 2022.

2.5.2. Uruguai

Em 29 de dezembro de 2022, pela Resolução nº 50/2022, a Unidade de Regulação e Controle de Dados Pessoais (URCDP) habilitou o uso das cláusulas da RIPD como opção para transferências internacionais de dados pessoais para países inadequados.

Esta Resolução indica que as cláusulas serão aplicadas com as correspondentes adaptações de acordo com as regulamentações nacionais, com exceção dos casos em que as cláusulas ofereçam maiores garantias aos titulares dos dados.

Deve ter-se em conta que, para estes efeitos, é necessária a autorização da Unidade de Regulação. Para a concessão dessa autorização, a URCDP terá em conta as SCCs como forma de oferecer garantias suficientes quanto à proteção da vida privada, dos direitos e liberdades fundamentais das pessoas, bem como no que respeita ao exercício dos respectivos direitos, que constituem garantias necessárias à aprovação de tais transferências internacionais de dados pessoais.

2.5.3 Argentina

A AAIP, por meio da Resolução 198/2023, aprovou as cláusulas-padrão contratuais para transferências internacionais de dados e o Guia de Implementação do RIPD. A Agência é membro do Comitê Executivo, com o objetivo de avançar para a convergência de ferramentas, simplificando procedimentos e estabelecendo pisos de garantia comuns que reforcem a confiança entre os países.

Nesse sentido, disse a chefe da AAIP, Beatriz Anchorena,

> Essas cláusulas são um instrumento para fortalecer a proteção de dados pessoais em fluxos transfronteiriços, quando um Estado não possui legislação adequada para transferências internacionais. Este é mais um passo para promover o desenvolvimento econômico e garantir a proteção de direitos.

As Cláusulas-padrão contratuais para transferências internacionais de dados foram desenvolvidas pelo RIPD como uma alternativa economicamente viável para que empresas ou organizações não precisem ne-

gociar acordos individuais. Este progresso está alinhado com o detalhado no Plano Estratégico de Proteção de Dados Pessoais 2022-2026 da AAIP e responde aos compromissos internacionais assumidos pela Argentina.

Desta forma, a Argentina torna-se o terceiro país da região a aprovar essas Cláusulas, juntamente com o Uruguai e o Peru.

2.5.4 Brasil

O Brasil realizou uma consulta pública durante 2023 e propôs a adoção de uma regulamentação expressa sobre a matéria do TIDP. Mas em anexo a essa proposta regulatória, a ANPD propôs uma minuta de cláusula contratual diferente do modelo RIPD, modelo que contempla algumas questões específicas da LGPD brasileira.

3 As cláusulas-padrão da Rede Ibero-Americana de Proteção de Dados

Dada a falta deste tipo de cláusula em nossa região, a Rede se propôs a desenvolver um guia para o uso de SCCs como alternativa para realizar transferências internacionais de dados pessoais.

O Guia para a Implementação de Cláusulas Contratuais Modelo para a Transferência Internacional de Dados Pessoais publicado pela RIPD prevê as SCCs correspondentes às transferências entre controlador e controlador e transferências entre controlador e operador.

Em 23 de novembro de 2021, a RIPD recebeu comentários e observações sobre o Guia de Implementação e os dois modelos de acordos internacionais de transferência entre controlador-controlador e controlador-operador. Ambos os documentos foram aprovados na sessão fechada da RIPD no final daquele ano.

3.1 Esboço das cláusulas contratuais da RIPD

As SCCs retiram as suas linhas gerais e a sua estrutura das SCCs aprovadas pela UE em junho de 2021. Mas, quanto ao seu conteúdo, eles se baseiam nos Padrões Ibero-Americanos de Proteção de Dados desenvolvidos

pela RIPD em 2017. Isso faz sentido, porque na América Latina não existe um direito comum de proteger dados pessoais para todos os países, como é o caso da UE. Por esta razão, a RIPD tomou como base as Normas que foram elaboradas em 2017 em resposta ao surgimento do GDPR e à necessidade de ter um direito substantivo comum em termos de dados pessoais.

3.2 Importância da adoção pelas autoridades da região

Embora os controladores e operadores sejam livres para usar essas SCCs para fornecer salvaguardas para transferências internacionais de dados pessoais, também é possível que as Autoridades competentes as incorporem como modelos seguindo as etapas correspondentes em seu sistema legal. Isso é possível porque, se as autoridades têm autoridade legal para decidir quando uma transferência é feita de acordo com a lei, elas também podem decidir com antecedência que o uso de certas SCCs é suficiente para cumprir sua legislação.

Para esse fim, seria possível emitir uma norma na qual as cláusulas contratuais padrão (com quaisquer alterações a serem feitas localmente) são consideradas como fornecedoras de salvaguardas adequadas para a transferência de dados pessoais por um controlador ou operador sujeito à sua lei local de proteção de dados pessoais (exportador de dados) para um controlador ou (sub)operador cujo tratamento de dados não está sujeito à lei local de proteção de dados pessoais (importador de dados).

Anexo A – Guia para Implementação de Cláusulas Contratuais Modelo da RIPD

Introdução

O uso de cláusulas contratuais é uma alternativa para poder realizar transferências internacionais de dados pessoais. A este respeito, o artigo 36(1)(c) das Normas de Proteção de Dados Pessoais para os Estados Ibero-Americanos da Rede Ibero-Americana de Proteção de Dados (RIPD) prevê que

> O responsável pelo tratamento e o processador podem realizar transferências internacionais de dados pessoais em qualquer um dos seguintes casos: (...) c. O exportador e o destinatário assinam cláusulas contratuais ou qualquer outro instrumento legal que ofereça garantias suficientes e que permita demonstrar o alcance do tratamento dos dados pessoais, as obrigações e responsabilidades assumidas pelas partes e os direitos dos titulares. A autoridade de controle pode validar cláusulas contratuais ou instrumentos legais conforme determinado na legislação nacional dos Estados Ibero-Americanos aplicáveis ao assunto.

Em consonância com o exposto, este guia procura estabelecer os principais aspectos que devem ser tidos em conta quando as transferências internacionais de dados pessoais (doravante TIDP) são efetuadas através da utilização de cláusulas contratuais modelo (doravante CCM). Como tal, este guia apresenta algumas orientações a serem levadas em consideração por aqueles que devem levar as TIDP a jurisdições inadequadas dos países-membros da Rede Ibero-Americana de Proteção de Dados Pessoais (RIPD).

Além disso, na América Latina não existem CCMs aprovadas conjuntamente a nível regional. Por esta razão, a RIPD apresenta como anexo a este Guia um modelo de contrato de transferência internacional em duas versões, uma para transferências entre Controladores e outra para transferências de Controladores para Processadores. Estes dois modelos são considerados como um primeiro passo e espera-se que modelos adi-

cionais sejam desenvolvidos em uma etapa posterior para transferências de Processador para Processador e de Processador para Responsável.

O conteúdo substancial de ambos os modelos segue as diretrizes das Normas de Proteção de Dados Pessoais para Estados Ibero-americanos da RIPD[88] ("Normas").

As CCMs propostas no Anexo também são semelhantes em sua estruturação com as recentes cláusulas contratuais padrão para a transferência de dados pessoais para países terceiros aprovados em junho de 2021 pela Comissão da União Europeia ("UE")[89], pois em sua essência contém elementos e princípios.

1 Precisões e limitações

Este Guia é complementar às recomendações, documentos e regulamentos vigentes em cada país da Ibero-América.[90] Os regulamentos de proteção de dados aplicáveis nos países da Ibero-América contêm disposições específicas relacionadas com as TIDP e vários incluem até mesmo uma disposição para o uso de cláusulas contratuais. Em alguns casos, foram desenvolvidos modelos próprios de cláusulas contratuais com base na legislação nacional (ver ponto 2.3. deste guia).

Este guia não substitui as regulamentações nacionais nem as diretrizes ou critérios expressos pelas diferentes autoridades de proteção de dados da região no exercício de seus poderes.

Deve ainda esclarecer-se que, em caso de manifesta contradição entre este documento e qualquer recomendação ou guia da autoridade nacional de proteção de dados, sugere-se seguir a recomendação da referida auto-

88 Cfr. Rede Ibero-Americana de Proteção de Dados -RIPD- (2017). Normas de proteção de dados pessoais para os Estados Ibero-americanos. Disponível em: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf.

89 Cfr. DECISÃO DE EXECUÇÃO DA COMISSÃO (UE) 2021/914, de 4 de junho de 2021, sobre cláusulas contratuais padrão para a transferência de dados pessoais para países terceiros, em conformidade com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Disponível em: https://eur-lex.europa.eu/ legal-content/ES/TXT/HTML/?uri=CELEX:32021D0914&from=EN#ntr2-L_2021199ES.01003701-E0002.

90 Por exemplo, veja os mencionados na seção Documentos consultados deste Guia.

ridade no entendimento de que cabe a essa entidade determinar as regras efetivar uma TIDP de acordo com a legislação aplicável.

Em qualquer caso, a aplicação deste guia e a utilização dos dois modelos contratuais anexos a este guia devem ser feitas em harmonia com as recomendações, resoluções e determinações das autoridades locais de proteção de dados e, sobretudo, com a legislação local.

Para a elaboração[91] deste documento, bem como da CCM, foram tomadas como referência as Normas de Proteção de Dados Pessoais dos Estados Ibero-americanos da RIPD[92] para estabelecer os princípios, termos, definições, obrigações do Responsável e do Processador e direitos dos titulares de dados pessoais. O guia e a CCM não transcrevem literalmente todos os aspectos dele, mas os princípios contidos nas Normas foram tomados como fonte de todos os princípios legais que devem ser aplicados em caso da TIDP. Portanto, este documento deve ser lido em conjunto e de forma abrangente com as Normas acima mencionadas, sem prejuízo de eventuais adaptações que possam ser feitas em nível nacional.

Este Guia não é um conceito jurídico, nem um artigo acadêmico, nem constitui aconselhamento jurídico de qualquer tipo. Tampouco pretende ser uma lista exaustiva de recomendações específicas, porque esta é uma questão interna que cada organização deve decidir à luz dos objetivos e da magnitude de cada projeto que envolve a transferência de dados pessoais para jurisdições inadequadas.

---

91 A Rede Ibero-Americana de Proteção de Dados (RIPD) agradece o trabalho realizado por Pablo Palazzi na elaboração deste guia e seu anexo. A RIPD publicou a versão anterior deste documento para comentários públicos. Comentários e sugestões foram recebidos e analisados das seguintes pessoas e organizações cuja participação agradecemos: (1) SEPD (Autoridade Europeia para a Proteção de Dados); (2) APEP (Associação Profissional Espanhola de Privacidade); (3) Gustavo Parra (Instituto de Transparência, Acesso à Informação Pública e Proteção de Dados Pessoais do Estado do México e Municípios); (4) A Associação Latino-Americana de Internet (ALAI), (5) Daniel Bulnes; (6) Associação de Internet MX; (7) Professora Lourdes Zamudio; (8) Equifax.

92 Cfr. Rede Ibero-Americana de Proteção de Dados -RIPD- (2017). Normas de proteção de dados pessoais para os Estados Ibero-americanos. Disponível em: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf.

2 Antecedentes da transferência internacional de dados pessoais (TIDP)

2.1 Antecedentes internacionais

A Diretiva de Proteção de Dados da União Europeia de 1995[93] foi o primeiro regulamento que implementou regras aplicáveis nas TIDP ao nível do direito comunitário europeu. A referida Diretiva foi revogada e substituída pelo 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 (doravante Regulamento Geral de Proteção de Dados, RGPD).[94]

O RGPD contém em seu quinto capítulo uma regulamentação detalhada das transferências internacionais de dados pessoais (Artigos. 44 a 50, RGPD). Art. 46 inc. 2º do RGPD permite a TIDP quando são adotadas garantias adequadas, entre as quais estão as cláusulas-padrão de proteção de dados aprovadas pela Comissão Europeia ou por alguma autoridade de controle.

Através da Decisão 2001/497/CE da Comissão[95] e depois através da Decisão 2010/87/UE da Comissão Europeia[96], foram aprovados dois modelos que contêm cláusulas contratuais padrão para facilitar a transferência de dados pessoais de um Responsável estabelecido na UE para outro Res-

93 Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (DO L 281 de 23.11.1995, p. 31). Disponível em https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A1995%3A281%3ATOC.

94 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, DO L 119 de 4.5.2016, p. 1. Disponível em https://eur-lex. europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC.

95 Decisão 2001/497/CE da Comissão, de 15 de junho de 2001, relativa às cláusulas contratuais padrão para a transferência de dados pessoais para um país terceiro previstas na Diretiva 95/46/CE. Disponível em https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A2001%3A181%3ATOC.

96 Decisão 2010/87/UE da Comissão, de 5 de fevereiro de 2010, relativa às cláusulas contratuais padrão para a transferência de dados pessoais para processadores de dados estabelecidos em países terceiros de acordo com a Diretiva 95/46/EC do Parlamento Europeu e do Conselho. Disponível em https://eur-lex.europa. eu/legal-content/ES/TXT/?uri=OJ%3AL%3A2010%3A039%3ATOC.

ponsável ou Processador estabelecido em um terceiro país que não oferece um nível adequado de proteção.

As cláusulas contratuais padrão das Deliberações mencionadas foram atualizadas em junho de 2021 para adequá-las ao RGPD, processo que incluiu consulta pública.[97] A nova decisão[98] aprova um modelo mais completo adaptado às alterações regulamentares e às novas formas de tratamento de dados pessoais.

Convém mencionar também o "Acordo de Comércio Eletrônico MERCOSUL"[99] (vinculante para a República da Argentina, a República Federativa do Brasil, a República do Paraguai e a República Oriental do Uruguai) assinado em 28 de janeiro de 2021.

O art. 6.2 do referido Contrato prevê que as partes devem adotar ou manter leis, regulamentos ou medidas administrativas para a proteção das informações pessoais dos usuários que participam do comércio eletrônico. Para tanto, levarão em consideração as normas internacionais existentes nesta matéria.

Também, o art. 6.7 do Acordo prevê que as partes se comprometam a aplicar um nível adequado de proteção aos dados pessoais que recebem de outra Parte por meio de uma regra geral ou regulamento autônomo específico ou por acordos mútuos, gerais ou específicos, ou em quadros internacionais mais amplos, admitindo para o setor privado a implementação de contratos ou autorregulação.

O art. 7º do regulamento do MERCOSUL estabelece o princípio da não discriminação em matéria de transferência internacional de dados pessoais.

---

97 Essas novas cláusulas contratuais receberam comentários, contribuições e sugestões de toda a comunidade internacional e constituem um texto que reflete as mais importantes normas internacionais, incluindo os mais recentes desenvolvimentos jurisprudenciais sobre o assunto.

98 DECISÃO DE EXECUÇÃO DA COMISSÃO (UE) 2021/914, de 4 de junho de 2021, sobre cláusulas contratuais padrão para a transferência de dados pessoais para países terceiros, em conformidade com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Disponível em: https://eur-lex.europa.eu/ legal-content/ES/TXT/HTML/?uri=CELEX:32021D0914&from=EN#ntr2-L_2021199ES.01003701-E0002.

99 Ver MERCOSUR/CMC/DEC. Nº 15/20. Disponível em: https://normas.mercosur.int/public/normativas/4018 e https://normas.mercosur.int/simfiles/normati-vas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.

Em 9 de abril de 2021, a Comissão Jurídica Interamericana da Organização dos Estados Americanos aprovou os Princípios Atualizados sobre Privacidade e Proteção de Dados Pessoais.[100]

O princípio n. 11 refere-se ao fluxo de dados transfronteiriço e fornece o seguinte:

> Reconhecendo seu valor para o desenvolvimento econômico e social, os Estados-membros devem cooperar entre si para facilitar o fluxo transfronteiriço de dados pessoais para outros Estados quando eles fornecem um nível adequado de proteção de dados de acordo com estes Princípios. Da mesma forma, os Estados-membros devem cooperar na criação de mecanismos e procedimentos que assegurem que os responsáveis e encarregados do tratamento de dados que operem em mais de uma jurisdição, ou os transmitam para uma jurisdição diferente da sua, possam garantir e ser efetivados responsável pelo cumprimento destes Princípios.

Por outro lado, a Convenção n. 108 do Conselho da Europa com as modificações do Protocolo de 2001[101] prevê em seu art. 2 intitulado "Transferência de dados pessoais para destinatários não sujeitos à jurisdição das Partes da Convenção" que "Cada Parte deverá prever que a transferência de dados pessoais para um destinatário sujeito à jurisdição de um Estado ou organização que não seja Parte à Convenção só será cumprida se o referido Estado ou organização assegurar um nível adequado de proteção".

O artigo 2.2 estabelece que "o artigo 2(1) do presente Protocolo não se aplica e as Partes podem autorizar a transferência de dados pessoais: (...) b) se forem fornecidas pelo responsável pela transferência garantias suficientes, que podem resultar, em particular, de cláusulas contratuais, pelo responsável pela transferência e se tais garantias forem consideradas adequadas pelas autoridades competentes de acordo com a legislação nacional".

---

100 OEA, Princípios atualizados sobre privacidade e proteção de dados pessoais, com anotações (CJI/RES. 266 (XCVIII-O/21)). Disponível em: http://www.oas.org/es/sla/ddi/ proteccion_ datos_personales_trabajos_actuales_CJI.asp.

101 Disponível em: https://rm.coe.int/1680080626.

2.2 Rede Ibero-Americana de Proteção de Dados

A RIPD com base no artigo 1, alínea a) do Regulamento da Rede Ibero-Americana de Dados Pessoais e com o objetivo de desenvolver e dispor de regulamentos que garantam o direito à proteção e privacidade de dados nos países da região; tem se preocupado com a regulamentação legal da TIDP desde o seu início. Assim, no marco do III Encontro Ibero-Americano sobre Proteção de Dados, realizado em Cartagena das Índias (Colômbia) em 2004,[102] os membros da RIPD emitiram várias conclusões onde era evidente sua preocupação com a TIDP.

Nessa reunião, os membros da RIPD concluíram que

> A transferência internacional de dados pessoais deve estar sujeita a um regime de garantias para evitar que os princípios que regem o direito fundamental à proteção de dados sejam violados pela mera transferência desses dados a outro país. A Diretiva de Proteção de Dados da União Europeia consagrou este princípio e deu à Comissão Europeia o poder de decidir que um país que estabeleceu legislação de proteção de dados de acordo com os padrões europeus e criou uma autoridade de controle independente é um destino seguro para dados pessoais de Estados-membros da UE.

No mesmo documento, os membros da RIPD esclareceram que

> Na ausência desse reconhecimento, é possível, entre outras opções, utilizar cláusulas contratuais padrão [...] Sua utilização permite estabelecer as garantias necessárias que compensam a falta de legislação adequada no país de destino, dando às pessoas cujos dados são transferidos a possibilidade de exigir o cumprimento das cláusulas do contrato que as afetam, bem como a reparação no caso de serem prejudicadas pelo não cumprimento.

A Declaração de Cartagena das Índias conclui afirmando que

> Assim, os participantes do III Encontro Ibero-Americano de Proteção de Dados esperam que nos países ibero-americanos se estabeleçam normas sobre proteção de dados e se estabeleçam mecanismos de controle independentes que promovam uma efetiva implemen-

102 RIPD, Declaração de Cartagena das Índias, maio de 2004, ponto III - "Transferências internacionais de dados. Perspectivas europeias e ibero-americanas". Disponível em: https://www.redipd.org/sites/default/files/inline-files/declaracion_2004_III_encuentro_es.pdf.

> tação do direito fundamental à proteção de dados pessoais que, ao mesmo tempo, facilita o livre fluxo de dados pessoais entre países.

No âmbito da XVIII Reunião Ibero-Americana sobre Proteção de Dados[103] realizada on-line em 4 de dezembro de 2020 em Montevidéu (Uruguai), os membros da RIPD estabeleceram em sua Declaração Final (ponto 7 da conclusão) que:

> o tratamento dos dados pessoais como motor da economia mundial requerem regras claras e transparentes que permitam fluxos de dados internacionais seguros, com base na consideração do nível de proteção fornecido pelos países ou organizações que são destinatários desses fluxos, em tratados internacionais ou em normas contratuais entre emitentes e destinatários que garantem a validade dos princípios de proteção de dados, o exercício dos direitos pelos titulares e o cumprimento das obrigações correspondentes aos responsáveis, encarregados do tratamento e outros terceiros.

Em conclusão, é natural que no desenvolvimento de documentos complementares às Normas e Declarações da RIPD, procuremos desenvolver guias e modelos que facilitem o livre fluxo de dados, mas mantendo a proteção adequada dos dados pessoais dos titulares, como as CCM ou códigos corporativos obrigatórios.

Em 2017, os membros da RIPD aprovaram as Normas de Proteção de Dados Pessoais para os Estados Ibero-americanos.

As Normas Ibero-Americanas procuram estabelecer um conjunto de princípios e direitos comuns de proteção de dados pessoais que os Estados Ibero-Americanos podem adotar e desenvolver em sua legislação nacional, a fim de ter regras homogêneas na região. Por outro lado, as Normas Ibero-Americanas incluem as melhores práticas nacionais e internacionais no campo no momento de sua emissão. Entre os objetivos das Normas Ibero-Americanas estão os seguintes, que de alguma forma justificam a adoção da CCM para a região: *i)* facilitar o fluxo de dados pessoais entre os Estados Ibero-Americanos e além de suas fronteiras, a fim de contribuir para o crescimento econômico e desenvolvimento social da região e *ii)* promover a cooperação internacional entre as autoridades de controle dos Estados

103 RIPD, XVIII Encontro Ibero-Americano de Proteção de Dados. Disponível em: https://www.redipd.org/sites/default/files/2020-12/declaracion-final-xviii-encuentro.pdf.

Ibero-Americanos, com outras autoridades de controle não pertencentes à região e autoridades e organismos internacionais na matéria.

Artigo 36 inc. 1, letra "c" das Normas estabelece que

> O responsável e o processador podem realizar transferências internacionais de dados pessoais em qualquer um dos seguintes casos: (...) c. O exportador e o destinatário assinam cláusulas contratuais ou qualquer outro instrumento legal que ofereça garantias suficientes e que permita demonstrar o alcance do tratamento dos dados pessoais, as obrigações e responsabilidades assumidas pelas partes e os direitos dos titulares. A autoridade de controle pode validar cláusulas contratuais ou instrumentos legais conforme determinado na legislação nacional dos Estados Ibero-Americanos aplicáveis ao assunto.

Das Normas Ibero-Americanas emerge o seguinte:

- O Exportador e o Importador podem firmar cláusulas contratuais.
- Estas cláusulas contratuais devem oferecer garantias suficientes que permitam demonstrar: *i)* o âmbito do tratamento dos dados pessoais; *ii)* as obrigações e responsabilidades assumidas pelas partes; e *iii)* os direitos dos Titulares.
- A respectiva autoridade de controle poderá validar cláusulas contratuais ou instrumentos legais conforme determinado na legislação nacional dos Estados Ibero-Americanos aplicáveis ao assunto.

2.3 Regulamentos Ibero-Americanos sobre TIDP

De acordo com as referidas normas internacionais e com as Normas, um grande número de países ibero-americanos regulamenta a transferência internacional de dados pessoais, na falta de continuidade no nível de proteção.

É o caso dos seguintes países:

- **Argentina** (art. 12 da Lei n. 25.326 de Proteção de Dados Pessoais, art. 12 do Decreto Regulamentar n. 1558/2001 e Disposição 60).
- **Brasil** (arts. 33 a 35 da Lei Geral de Proteção de Dados).
- **Cabo Verde** (art. 20º, Lei nº 41/VIII/2013, de 17 de setembro, sobre a Proteção de Dados Pessoais de Pessoas Naturais).

- **Colômbia** (art. 26 da Lei 1.581 de 2012).
- **Equador** (arts. 55 a 61 da Lei Orgânica de Proteção de Dados Pessoais).
- **México** (arts. 65 a 71 da Lei Geral de Proteção de Dados Pessoais detidos por Pessoas Jurídicas e artigos. 36 e 37 da Lei Federal de Proteção de Dados Pessoais detidos por Particulares).
- **Nicarágua** (art. 14 da Lei nº 787, Lei de Proteção de Dados Pessoais).
- **Panamá** (arts. 5 e 33, Lei nº 81, de 26 de março de 2019, de Proteção de Dados Pessoais e artigos. 51 a 53 do Decreto Executivo nº 285 de 28 de maio de 2021).
- **Peru** (arts. 11 e 15 da Lei 29.733, Lei de Proteção de Dados Pessoais).
- **República Democrática de São Tomé e Príncipe** (arts. 19 e 20, Lei 3/2016, de 2 de maio, Proteção de Dados Pessoais de Pessoas Físicas).
- **República Dominicana** (art. 80 da Lei nº 172-13, de 13 de dezembro de 2013, de Proteção de Dados Pessoais).
- **Uruguai** (art. 23 da Lei nº 18.331 de Proteção de Dados Pessoais, Resolução nº 4/019, de 12 de março de 2019 e Resolução nº 41/021, de 8 de setembro de 2021).

A maioria das legislações acima mencionadas também prevê certas exceções para permitir que a TIDP tenha destinos impróprios (por exemplo, onde existam tratados internacionais). Por outro lado, também é possível recorrer a outras ferramentas para transferência internacional. Por exemplo, as regulamentações da Argentina, Colômbia,[104] México,[105]

104 Colômbia: Em sua nova versão do ano de 2021, o Guia emitido pela autoridade colombiana para a proteção de dados pessoais fornece diretrizes sobre a TIDP e o uso da CCM. Ver Colômbia, SIC, Guia para a implementação do princípio da responsabilidade demonstrada nas transferências internacionais de dados pessoais, p. 17, onde se recomenda a utilização de cláusulas contratuais para a TIDP como forma de demonstrar a responsabilização do Responsável pelo tratamento dos dados pessoais. Disponível em: https://www.sic.gov.co/sites/default/files/files/2021/2021%20Gu%C3%ADAs%20para%20implementaci%C3%B3n%20del%20 principio%20de%20responsibility%20demonstrada% 202021.pdf.

105 México, o artigo 75 do Regulamento da Lei Federal de Proteção de Dados Pessoais de Titularidade Privada (LFPDPPP), sugere as cláusulas contratuais, ao prever "Para este fim, o responsável que transfere os dados pessoais pode usar cláusulas contratuais ou outros instrumentos legais que

Panamá,[106] Peru[107] e Uruguai contemplam ou recomendam a possibilidade de utilização da CCM.

Por sua vez, algumas autoridades de proteção de dados, como Uruguai e Argentina, emitiram regulamentos que aprovam diretrizes ou modelos de CCM.[108]

3 Principais atores da TIDP

Os principais atores envolvidos na TIDP são apresentados a seguir. Isso ajuda a entender o interesse de cada parte em uma TIDP.

As TIDPs ocorrem em muitas situações como: transferências bancárias, reservas de passagens aéreas e hotéis, serviços de computação em nuvem, centralização de recursos humanos, operações tradicionais de comércio exterior e comércio eletrônico, entre muitos outros casos.

No cenário típico de uma TIDP (seja qual for o motivo), temos os seguintes elementos e atores:

---

prevejam, pelo menos, as mesmas obrigações a que está sujeito o responsável pela transmissão dos dados pessoais, bem como as condições em que o titular consentiu no tratamento dos seus dados pessoais. Por outro lado, o Artigo 66 da Lei Geral de Proteção de Dados Pessoais na Posse de Sujeitos Obrigados, que estabelece que "Todas as transferências devem ser formalizadas através da assinatura de cláusulas contratuais, acordos de colaboração ou qualquer outro instrumento legal, de acordo com os regulamentos aplicáveis ao responsável pelo tratamento de dados, que permitam demonstrar o alcance do tratamento de dados pessoais, assim como as obrigações e responsabilidades assumidas pelas partes". Deve-se esclarecer que no México existe uma Lei aplicável a pessoas físicas e outra para Sujeitos Obrigados, que oportunamente são aquelas instituições de natureza pública.

106 Panamá, Art. 53 inc. 2º do Decreto Executivo nº 285 de 18 de maio de 2021. Disponível em https://www.gacetaoficial.gob.pa/pdfTemp/29296_A/GacetaNo_29296a_20210528.pdf.

107 Peru, o artigo 25 do Regulamento LPDP, também considera as cláusulas contratuais, quando afirma que "o emissor ou exportador pode usar cláusulas contratuais ou outros instrumentos legais que estabeleçam pelo menos as mesmas obrigações a que está sujeito, bem como as condições em que o titular consentiu no tratamento dos seus dados pessoais.

108 Uruguai: Resolução nº 41/021, de 8 de setembro de 2021. Disponível em https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/noticias/changes-regimen-transferencias-internacionales-datos-uruguay e Argentina: Disposição 60/2016 da Direção Nacional de Proteção de Dados Pessoais. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/texact.htm.

- Uma entidade que deseja enviar dados para o exterior nomeada: Exportador de dados.
- Uma entidade que deseja receber esses dados nomeada: Importador de dados, localizado em outra jurisdição.
- O Importador recebe os dados para tratá-los com uma determinada finalidade. Mas a TIPD é em si um tratamento de dados: supõe-se que qualquer transferência internacional de dados pessoais TIPD implica o tratamento de dados de acordo com a definição dada pelas Normas.[109]
- O Titular dos dados pessoais é a "pessoa singular a quem os dados pessoais se referem"[110] cujas informações devem ser processadas adequadamente. Todos os direitos do Titular devem ser garantidos quando o tratamento for realizado por meio de um TIDP para uma jurisdição caracterizada como não adequada. No caso das Normas, os direitos a serem garantidos são mencionados nos artigos 24 a 32. Uma forma de garantir esses direitos é através do uso da CCM.
- Por sua vez, o Titular é um Terceiro Beneficiário na CCM. Isso significa que o Titular tem direitos que derivam não apenas da lei de proteção de dados pessoais da jurisdição do Exportador de Dados, mas também do contrato de transferência internacional firmado entre as partes (ver ponto 7 deste Guia).
- Uma jurisdição inadequada onde o Importador de Dados está localizado. Esta jurisdição é caracterizada como não adequada para fins da TIDP de acordo com a regulamentação do país do Exportador de Dados ou a interpretação da Autoridade competente. A falta de adequação da jurisdição de destino obriga as partes a adotarem salvaguardas que proporcionem garantias adequadas à proteção dos dados sujeitos a TIDP, por exemplo, através da assinatura da CCM.

109 Cf. literal i do art. 2 das Normas de Proteção de Dados Pessoais dos Estados Ibero-Americanos (2017).

110 Cfr. Artigo 2.1(h) das Normas de Proteção de Dados Pessoais para os Estados Ibero-Americanos (2017).

- A autoridade de proteção de dados (Autoridade de Controle)[111] deve garantir que aqueles que realizam a TIDP realizam essa atividade, observando o disposto na regulamentação sobre o assunto.
- Lei aplicável: Os regulamentos sobre transferência internacional de dados ou "fluxo de dados transfronteiriço" procuram garantir que o nível de proteção dos dados pessoais dos cidadãos de um país não diminua ou desapareça quando estes devem ser exportados ou transferidos para outro ou outros países[112]. Como consequência da necessidade de proteger os dados pessoais transferidos para uma jurisdição não adequada, é necessário que os dados pessoais estejam sujeitos a uma proteção semelhante àquela existente no momento da coleta.

3.1 Vejamos um exemplo com o cenário de processamento de dados por meio de serviços de computação em nuvem de acordo com as diretrizes aprovadas pela RIPD sobre o assunto

Em abril de 2020, a RIPD publicou as "Recomendações para o processamento de dados pessoais por meio de serviços de computação em nuvem."[113] Neste documento, a RIPD concluiu que o processamento de dados pessoais na nuvem pode envolver a transferência internacional de dados pessoais.[114] As recomendações contêm sugestões para que os prestadores de serviços de computação em nuvem (PSCEN) possam prestar os seus serviços respeitando os direitos de dados pessoais dos Titulares e as regras da TIDP.

111 O Capítulo VII das Normas estabelece os principais aspectos das autoridades de controle e supervisão da proteção de dados.

112 Consulte RIPD, Recomendações para o processamento de dados pessoais por meio de serviços de computação em nuvem. Disponível em https://www.redipd. org/sites/default/files/2021-06/recomendaciones-tratamiento-datos-personales-servicios-nube.pdf.

113 Idem.

114 RIPD, Recomendações para o tratamento de dados pessoais através de serviços de computação em nuvem, p. 15.

Em suas Recomendações, as RIPD afirmam o seguinte: "Se os 'datacenters' ou equipamentos de armazenamento PSCEN estiverem localizados fora do país onde está localizada a parte contratante dos serviços de computação em nuvem (CEN), os dados pessoais serão enviados ou exportados de um país para empresas e organizações PSCEN localizadas em um território diferente do país remetente. É um processo de exportação de dados pessoais".

Após essa explicação, o documento especifica: "Neste caso, a empresa contratante dos serviços do CEN será o Exportador e o PSCEN atuará como destinatário da referida exportação de dados. As Normas definem o Exportador como a "pessoa física ou jurídica de natureza privada, autoridade pública, serviços, órgão ou prestador de serviços situado no território de um Estado que realiza transferências internacionais de dados pessoais, de acordo com o disposto nestas Normas". Assim, o contratante dos serviços do CEN deve observar as regras locais de transferência internacional de dados".

As mencionadas Recomendações da RIPD concluem que "É importante que o contratante dos serviços do CEN esteja plenamente ciente e, se for o caso, possa aceitar ou limitar os países em que os servidores serão hospedados, além de ser informado das devidas salvaguardas adotadas."

Tudo isso é explicado com a base da TIDP: "Os regulamentos sobre transferência internacional de dados ou "fluxo de dados transfronteiriço" procuram garantir que o nível de proteção dos dados pessoais dos cidadãos de um país não diminua ou desapareça quando estes devem ser exportados ou transferidos para outro ou outros países. Esta regra é conhecida como princípio da continuidade da proteção de dados, que se baseia no fato de que a transferência internacional de dados não deve afetar a proteção das partes interessadas no que diz respeito ao tratamento de seus dados pessoais. A exportação de informações pessoais não pode se tornar um cenário que reduza o nível de proteção conferido ao titular dos dados no país de onde os dados pessoais são exportados. Essas atividades não devem facilitar, permitir ou tolerar a violação dos direitos dos indivíduos ou a redução das garantias de que dispõem no país exportador. Nesse sentido, devem ser observadas as regras de transferências internacionais que vigoram no país do contratante dos serviços do CEN. No caso das Normas, o artigo 36 prevê as alternativas permitidas para exportar os dados."

No caso específico analisado, a empresa contratante dos serviços do CEN será a Exportadora de Dados e a PSCEN será a Importadora de Dados. Ambas as partes podem assinar um contrato com base na CCM em que o Importador de Dados atua como Processador usando o respectivo modelo da CCM.

4 Regra geral na TIDP – exceções e mecanismos de transferência mais usados

4.1 Regra Geral

As disposições sobre TIDP contidas nas leis de proteção de dados dos países ibero-americanos visam garantir a continuidade do nível de proteção previsto em suas leis quando houver uma transferência de dados pessoais para um terceiro país considerado inadequado ou que tenha um nível diferente de proteção de dados pessoais.

Os países podem reconhecer outras jurisdições como "adequadas" à sua legislação de dados pessoais, dependendo do nível de proteção garantido pela legislação aplicável. Em virtude do princípio geral de proibição do TIDP, na ausência de uma decisão de adequação ou referência específica no país exportador de dados, o Responsável ou o Processador só poderá transferir dados pessoais para um terceiro país se tiverem sido oferecidas garantias adequadas e em condição de que os Titulares tenham direitos exigíveis e ações judiciais efetivas para proteger seus direitos. Tais garantias podem ser prestadas, entre outros meios, pelas Normas Corporativas Vinculativas (NCV)[115] ou pela CCM.

Em termos gerais, um país é considerado adequado quando possui determinados elementos em seu ordenamento jurídico que permitem concluir que os dados pessoais estão adequadamente protegidos. Por exemplo,

115 As Regras Corporativas Vinculativas são uma das salvaguardas apropriadas reconhecidas pela RGPPD e são definidas como "as políticas de proteção de dados pessoais empreendidas por um responsável ou processador estabelecido no território de um Estado-membro para transferência ou conjunto de transferências de dados pessoais a um responsável ou processador em um ou mais países terceiros, dentro de um grupo de empresas ou de um grupo de empresas envolvidas em uma atividade econômica conjunta" (Art. 4. 20) RGPD).

de acordo com os regulamentos da União Europeia, os seguintes elementos geralmente são avaliados para determinar o nível de adequação:

- O "Estado de Direito", o respeito aos direitos humanos e aos direitos fundamentais naquele ordenamento jurídico.
- Legislação atual, geral e setorial, sobre dados pessoais.
- As medidas de segurança aplicadas.
- As regras sobre transferências posteriores de dados pessoais para outro país terceiro ou organização internacional observadas nesse país.
- Direitos reconhecidos aos titulares de dados pessoais por meio de recursos administrativos e ações judiciais efetivas.
- A existência e o funcionamento efetivo de uma ou mais autoridades de controle independentes no país terceiro.
- Os compromissos internacionais assumidos pelo país terceiro ou outras obrigações decorrentes de acordos ou instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, nomeadamente em relação à proteção de dados pessoais.
- O acesso das autoridades públicas do país de destino aos dados transferidos e, de forma mais geral, o regime de exceções às regras de proteção de dados pessoais aplicáveis no país de destino.

4.2 Exceções

As Normas estabelecem no Art. 36.2 que a legislação nacional aplicável dos Estados Ibero-Americanos pode estabelecer expressamente limites às transferências internacionais de categorias de dados pessoais por razões de segurança nacional, segurança pública, proteção da saúde pública, proteção dos direitos e liberdades de terceiros, bem como por razões de interesse público.

Numerosos regulamentos contêm exceções à regra que proíbe a TIDP para países ou jurisdições inadequados. As regras das jurisdições ibero-americanas mencionadas no ponto 3.3 deste Guia contêm exceções individuais baseadas nesses princípios mencionados nas Normas. As exceções

são, por exemplo, o consentimento do envolvido, o interesse público, a execução ou conclusão de um contrato ou os interesses vitais do envolvido.

Um ponto importante a ter em mente é que estas exceções para a TIDP não podem ser aplicadas continuamente para todos os tipos de transferências, mas devem, devido à sua natureza excepcional, ser destinadas a uma transferência específica e direcionada.

4.3 Mecanismos de transferência

Caso o país de destino da TIDP não possua um nível adequado de proteção reconhecido, então a TIDP pode ser realizada por meio de mecanismo de transferência que conceda garantias adequadas, ou pela aplicação de alguma das exceções previstas na regulamentação local.

Os mecanismos TIDP que fornecem garantias adequadas são geralmente os seguintes:

- Cláusulas contratuais modelo (CCM).
- Normas societárias vinculantes (NCV).
- Código de conduta aprovado de acordo com a legislação aplicável.
- Mecanismo de certificação.
- Instrumentos juridicamente vinculativos e executáveis entre autoridades ou órgãos públicos.

A função das CCMs padrão é garantir que haja garantias adequadas de proteção de dados nas transferências internacionais de dados para jurisdições que não possuem um nível adequado de proteção reconhecido. O Exportador de Dados que transfere os dados pessoais para um terceiro país e o Importador de Dados que recebe os dados pessoais podem assinar um acordo para garantir os direitos dos titulares dos dados através da CCM.

Embora as CCM devam, em princípio, ser utilizadas para transferências para jurisdições inadequadas, a RIPD recomenda sua aplicação a todos os tipos de transferências internacionais, quando relevante para garantir a conformidade com os princípios de proteção de dados pessoais.

Finalmente, é importante observar que o uso da CCM não implica, em todos os casos, o pleno cumprimento da legislação ou regulamentos de

proteção de dados pessoais das jurisdições afetadas pela transferência e, portanto, exigências específicas devem ser seguidas[116].

5 As cláusulas contratuais modelo (CCM) como mecanismo de proteção da TIDP

5.1 Objetivo das CCM

O objetivo das CCM é garantir e facilitar o cumprimento dos requisitos previstos pela lei de proteção de dados do país do Exportador de Dados para a transferência de dados pessoais para um terceiro país que não tenha sido reconhecido com um nível de proteção adequado. A ideia é que a proteção inicialmente concedida aos dados pessoais permaneça presente independentemente de onde esses dados estejam localizados.

É por isso que as transferências subsequentes também são regulamentadas com precauções para evitar a redução do nível de proteção. Os Titulares estão envolvidos através de um conceito universal de direito contratual chamado de Beneficiário de Terceiros. E regulamenta o acesso das autoridades públicas na jurisdição do importador de dados que pode afetar os direitos da pessoa em questão.

5.2 Vantagens e benefícios das CCM

O uso de cláusulas contratuais modelo pode ajudar a superar possíveis limitações nas transferências de dados resultantes de diferenças no nível de proteção entre diferentes países. O instituto do contrato está presente em todos os ordenamentos jurídicos ibero-americanos e serve para comprometer o Importador de Dados a respeitar os dados pessoais do Proprietário, uma vez que os dados pessoais estejam na jurisdição de destino.

Em outras palavras: as cláusulas-modelo ou cláusulas-padrão contribuem para construir a convergência em nível contratual, criando um regime autônomo de proteção de dados, sem necessariamente exigir con-

116 Por exemplo, no caso do setor público no México, quando são realizadas transferências de dados pessoais que não possuem um nível de proteção adequado, uma Avaliação de Impacto na proteção de dados pessoais deve ser submetida previamente.

vergência em nível de país (neste caso, podem ir além do nível de proteção em determinados países).

Ao mesmo tempo, a expansão dos princípios de proteção de dados pessoais por meio de redes de contratos internacionais tem um forte impacto na convergência geral na região, pois estabelecem padrões comuns com os quais as empresas se familiarizam. Isso facilita no futuro o alinhamento da legislação nacional com as normas e padrões internacionais de proteção de dados pessoais.

Por outro lado, a utilização da CCM serve para garantir os princípios e deveres na proteção dos dados pessoais. Isso, por sua vez, leva à transparência, segurança jurídica e, portanto, previsibilidade, uma vez que:

1. Através de sua natureza vinculativa e executável como parte de um contrato, podem assegurar a continuidade da proteção quando os dados viajam ao exterior, e o fazem de uma forma que proporciona segurança jurídica;
2. Ao fazê-lo de forma clara e transparente, ajudam a construir confiança, o que por sua vez dá às empresas que utilizam tais cláusulas uma vantagem competitiva sobre aquelas que têm que recorrer a outros métodos.

As CCM servem para proteger a parte "mais fraca", que, obviamente, são as pessoas físicas cujos dados pessoais, sob a TIDP, são processados tanto pelo Exportador de Dados quanto pelo Importador de Dados.

Finalmente, o uso da CCM também permite uma solução particularmente econômica para o problema da TIDP; a razão é que as empresas não precisam negociar acordos em cada caso individual com o custo econômico em termos de representação legal e de tempo que isso implica. A existência da CCM permite-lhes contar com o modelo pré-aprovado pela Autoridade de Controle competente, sabendo que ao fazê-lo cumprem as suas obrigações legais relativas à transferência internacional de dados pessoais com uma solução simples e prática. Essa é uma grande diferença em relação a outras ferramentas, como mecanismos de certificação ou NCVs, que exigem um processo de certificação muitas vezes demorado e caro.

Em comparação com esses mecanismos, as CCMs são um instrumento "pronto para usar" e "pronto para implementar." Isto é particularmente

importante para as pequenas e médias empresas que não podem arcar com outras opções de implementação mais dispendiosas e demoradas.

É por isso que as CCMs são o mecanismo legal mais acessível e usado hoje para TIDP para jurisdições não adequadas. Estima-se que cerca de 80 a 90% das empresas que implementam mecanismos de TIDP utilizam a CCM como solução[117]. Isto, naturalmente, implica que as Partes de uma TIDP usando uma CCM não devem se limitar à exigência formal de sua assinatura, mas devem estar sempre preparadas para serem "responsáveis" por seu processamento de dados pessoais perante a autoridade supervisora competente e aos Sujeitos dos Dados e serem capazes de demonstrar o pleno cumprimento da lei aplicável e das obrigações impostas na CCM.

6 Questões práticas na implementação e execução das CCM

6.1 Aspectos gerais

Dada a multiplicidade de leis existentes na Ibero-América, este Guia baseia-se nas Normas aprovadas na XV Reunião desta Rede, realizada em Santiago do Chile, Chile, em 22 de junho de 2017. Também foram considerados os trabalhos realizados com a CIJ da OEA para a modernização dos princípios de privacidade elaborados pela referida organização, bem como o RGPD e a Convenção 108 modernizada.

As definições da CCM são retiradas das Normas. O mesmo se aplica às obrigações substantivas decorrentes das CCMs. Da mesma forma, foram consultados os modelos de cláusulas contratuais aprovados pela UE, bem como os modelos propostos pelas autoridades neozelandesas.

117 Um estudo realizado calcula que cerca de 85% utilizam CCM como mecanismos da TIDP. Veja Nigel Cory, Ellysse Dick, Daniel Castro, The Role and Value of Standard Contractual Clauses in EU-US Comércio Digital, ITIF, 17 de dezembro de 2020. Disponível em: https://itif.org/publications/2020/12/17/role-and-value-standard-contractual-clauses-eu-us-digital-trade. No mesmo sentido: Laura Bradford, Mateo Aboy, Kathleen Liddell, Cláusulas contratuais padrão para transferências transfronteiriças de dados de saúde após Schrems II, publicadas no *Journal of Law and the Biosciences*, v. 8, n. 1, 2021. Disponível em: https://doi.org/10.1093/jlb/lsab007.

6.2 Características das CCM: forma de uso

Os dois modelos das CCM incluídos no Anexo a este Guia caracterizam-se pelo seguinte:

- AS CCM do Anexo contêm dois modelos para as diferentes premissas da TIDP:

  i) Responsável para Responsável e ii) Responsável para Processador.

- É incluída uma primeira folha ou capa onde são inseridos todos os dados das partes e do contrato e seus endereços. A ideia é que, em princípio, não seja necessário modificar em nada o texto da CCM.
- As CCMs têm vários anexos para identificar as novas partes que aderem ao contrato após sua assinatura inicial pelo Importador e Exportador de Dados (Anexo A), os dados pessoais envolvidos nas transferências e seus objetivos (Anexo B), as medidas de segurança (Anexo C), a lista de sub-processadores no caso do segundo modelo (Anexo D) e documentação legal adicional que as partes podem desejar incluir, como avisos de privacidade ou políticas de privacidade (Anexo E).
- Com respeito ao Anexo A, cada nova Parte que aderir às CCMs deve assinar um Anexo separado e indicar o tipo de atividade que irá empreender com respeito às TIDP.
- Relativamente ao Anexo B, deve ser possível distinguir claramente a informação aplicável a cada transferência ou categoria de transferências.
- Em relação ao Anexo C, as medidas de segurança devem ser detalhadas com precisão. Não é possível incluir generalidades.
- Com relação ao Anexo D, deve-se mencionar os subdepartamentos caso você tenha optado por listá-los antecipadamente.

Além disso, considera-se importante ressaltar que o uso de CCMs requer verificação prévia das exigências da transferência no caso específico, e das características das entidades ou pessoas que as realizam, já que as

CCMs poderiam eventualmente incorporar elementos adicionais dependendo dessas suposições e das exigências regulatórias aplicáveis em cada um dos países onde tal processamento é realizado.

6.3 Posição das partes – incorporações de novas partes e utilização da CCM com outros acordos; modificações

Embora geralmente se faça referência a cláusulas contratuais padrão ou CCM, o termo refere-se a um modelo de contrato completo que pode ser utilizado tal qual ou modificado em aspectos secundários, desde que sua essência, que é a proteção dos direitos do Titular, não seja alterada de acordo com os regulamentos aplicáveis. É então possível acrescentar estes CCMs como um anexo a um contrato que as partes assinarão ou já assinaram, mas elas devem então realmente executar estes modelos para que sejam válidos e efetivos.

As partes têm a discrição de incluir em um contrato mais amplo tais cláusulas contratuais padrão, bem como de acrescentar cláusulas ou garantias adicionais, desde que não contradigam, alterem ou modifiquem direta ou indiretamente as cláusulas contratuais padrão ou prejudiquem os direitos fundamentais dos Titulares.

6.4 Lei aplicável às TIDP

A implementação da CCM ocorre quando uma entidade deve transferir dados para outra entidade localizada em outro país que não tenha sido reconhecido como país com nível de proteção adequado pelo país de origem. As Cláusulas Contratuais Modelo podem ser usadas em relação a tais transferências na medida em que o Importador de Dados esteja em um terceiro país que não seja o Exportador de Dados.

Em uma situação normal, cada parte estaria sujeita no processamento de dados pessoais transferidos às leis de seu respectivo país. No entanto, em questões da TIDP através da CCM, a lei aplicável (definida na CCM como "Lei Aplicável") é a lei do país ou jurisdição do Exportador de Dados.

A exportação de informações pessoais não pode se tornar um cenário que reduza o nível de proteção que é conferido ao Titular dos dados no país de onde os dados pessoais são exportados. A TIDP não deve facilitar ou permitir a violação dos direitos dos Titulares ou a redução das garantias de que dispõem os Titulares no país exportador[118]. Isto se baseia na lógica de que os dados são coletados e processados sob a lei do exportador de dados e quando são transferidos ao exterior para um país que foi reconhecido como tendo um nível de proteção adequado, é necessário preservar o nível de proteção que os dados pessoais têm no país de origem.

6.5 Cumprimento das normas gerais de proteção de dados pessoais

Além de utilizar o CCM para fornecer salvaguardas adequadas para transferências internacionais de dados pessoais, o Exportador de Dados tem que cumprir com suas obrigações gerais como Responsável ou Processador sob a lei de proteção de dados pessoais em vigor em sua jurisdição.

Entre essas responsabilidades, estão a obrigação do responsável de comunicar claramente aos Titulares em sua política de privacidade, a existência de transferências internacionais de seus dados pessoais para um terceiro país que não tenha um nível de proteção adequado reconhecido.

Além disso, é importante levar em consideração que, em conformidade com os deveres e princípios e obrigações referentes à proteção de dados pessoais no marco regulatório de cada país, pode haver exigências complementares, como no caso do México, onde existe a obrigação de comunicar a nota de privacidade. Portanto, aqueles requisitos que não são considerados na CCM devem ser adicionados nos anexos correspondentes, de forma a cumprir os princípios de informação e transparência do tratamento de dados pessoais.

6.6 Transferências subsequentes

Se o Importador precisar transferir os Dados Pessoais para outra entidade após receber os dados do Exportador, ocorre uma Transferência subsequente e é necessário continuar protegendo os dados pessoais.

118 RIPD, Recomendações para o tratamento de dados pessoais através de serviços de computação em nuvem, p. 15.

As transferências subsequentes pelo Importador de Dados para um terceiro em outro país terceiro só devem ser permitidas se esse terceiro aderir aos CCMs de teor semelhante e se a continuidade da proteção for assegurada de outra forma ou em situações específicas cobertas pelas CCMs.

Vale lembrar que cada vez que ocorre uma Transferência Subsequente no sentido acima definido, é atualizada a presunção de participação de um terceiro que, fazendo parte do tratamento, adquire responsabilidades em termos de proteção de dados pessoais. Em tal caso, seria necessário o acréscimo às Cláusulas Contratuais Modelo, seja assinando uma nova CCM individual com o Importador de Dados ou através de um instrumento legal específico.

6.7 Beneficiários de terceiros

Na CCM, o Titular é um Terceiro beneficiário do contrato modelo assinado pelas Partes. Em caso de violação de obrigações contratuais pelo Importador de Dados, o Sujeito de Dados poderá, como terceiro beneficiário, reclamar contra o Importador de Dados ou o Exportador de Dados por tal violação. Isso ocorre porque ambas as Partes fazem uma estipulação em favor do Titular.[119]

O princípio do Terceiro Beneficiário está contemplado na maioria dos códigos de direito privado latino-americanos. Assim, entre outros, encontramos nos códigos civis da Argentina (art. 1027 do Código Civil e Comercial da Nação), Bolívia (arts. 526 a 529 do Código Civil), Brasil (arts. 436 a 438 do Código Civil), Chile (art. 1449 do Código Civil), Colômbia (art. 1506 do Código Civil), Costa Rica (art. 1026 do Código Civil da Costa Rica), Equador (art. 1465 Código Civil), El Salvador (art. 1320 Código Civil), Guatemala (art. 1531 Código Civil), Honduras (art. 740 Código Comercial), México (arts. 1868-1871 do Código Civil Federal), Nicarágua (art. 1875 Código Civil), Paraguai (art. 732 do Código Civil), Peru (arts. 1457-1459 do Código Civil) e Uruguai (art. 1256 do Código Civil).

119 A estipulação ou contrato em favor de um terceiro é um acordo pelo qual uma parte (chamada de promotor) se compromete a outra (a parte estipuladora) a dar algo a um terceiro (ou beneficiário) ou a fazer ou não fazer algo em favor do terceiro, que, embora não seja parte do contrato, adquire os direitos nele mencionados.

6.8 Responsabilidade demonstrada

O artigo 20 das Normas[120] estabelece o princípio de responsabilidade (*accountability*). A norma prevê que o responsável implementará os mecanismos necessários para comprovar o cumprimento dos princípios e obrigações estabelecidos nas Normas, bem como prestar contas do tratamento dos dados pessoais em sua posse ao titular e à autoridade de controle, para o qual poderá recorrer a normas, melhores práticas nacionais ou internacionais, esquemas de autorregulação, sistemas de certificação ou qualquer outro mecanismo que considere adequado para tais fins.

120 Artigo 20 das Normas de Proteção de Dados Pessoais dos Estados Ibero-americanos (2017).

Anexo C – Modelos de Cláusulas Contratuais

1 Acordo modelo de transferência internacional de dados pessoais entre responsável e responsável

As Partes do Contrato concordaram com o presente Acordo com base em cláusulas contratuais modelo:

Primeira parte: questões gerais

Cláusula 1. Finalidade, partes, âmbito de aplicação e definições

1.1. Finalidade

A finalidade das presentes cláusulas contratuais modelo é garantir e facilitar o cumprimento dos requisitos previstos pela Lei aplicável para a transferência internacional de Dados Pessoais, com o intuito de cumprir os princípios e deveres na proteção dos Dados Pessoais e os direitos dos Titulares.

a. Qualquer interpretação do presente Acordo deverá levar em consideração tais propósitos.

1.2. Partes do contrato

a. As Partes do contrato são o Exportador de dados e o Importador de dados.

b. O presente Acordo permite a incorporação de importadores ou exportadores adicionais como Partes mediante o formulário do Anexo A seguindo o procedimento previsto na Cláusula 5.

1.3 Âmbito de aplicação

a. O presente Acordo será aplicado às transferências internacionais de Dados pessoais realizadas entre o Exportador de dados e o Importador de dados de acordo com as especificações do Anexo B.

b. Todos os anexos fazem parte do presente Acordo.

1.4. Definições

a. Os termos definidos são identificados neste Acordo com sua inicial em letra maiúscula.

b. Para efeitos do presente Acordo se entenderá por:

Acordo: o presente contrato de transferência internacional de Dados pessoais com base nas cláusulas contratuais modelo, juntamente com sua capa e seus anexos.

Anonimização: a aplicação de medidas de qualquer natureza destinadas a impedir a identificação ou reidentificação de uma pessoa física sem esforços desproporcionados.

Autoridade de controle competente: autoridade de proteção de dados pessoais do país do Exportador ou do Importador de dados pessoais.

Computação na nuvem: modelo para habilitar o acesso a um conjunto de serviços computacionais (p. ex. redes, servidores, armazenamento, aplicativos e serviços) de forma conveniente e sob demanda, que pode ser rapidamente provisionado e liberado com um esforço administrativo e uma interação com o provedor dos serviços.

Consentimento: manifestação da livre, específica, inequívoca e informada vontade do titular através da qual ele aceita e autoriza o tratamento dos dados pessoais relativos a ele.

Dados Pessoais: quaisquer informações relativas a uma pessoa física identificada ou identificável, expressa em forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica ou qualquer outro tipo. Considera-se que uma pessoa é identificável quando sua identidade pode ser determinada direta ou indiretamente, desde que isso não exija prazos ou atividades desproporcionais.

Dados pessoais sensíveis: aqueles que se refiram à esfera íntima de seu titular, ou cujo uso impróprio possa dar origem a discriminação ou

implicar um sério risco para este. De forma enunciativa, são considerados sensíveis os dados pessoais que possam revelar aspectos como origem racial ou étnica; crenças ou convicções religiosas, filosóficas e morais; afiliação sindical; opiniões políticas; dados relativos à saúde, à vida, preferência ou orientação sexual, dados genéticos ou dados biométricos destinados a identificar de forma unívoca uma pessoa física.

Decisões individuais automatizadas: decisões que produzam efeitos legais ao Titular ou o afetem significativamente e que se baseiam unicamente em tratamentos automatizados destinados a avaliar, sem intervenção humana, certos aspectos pessoais dele ou analisar ou prever, em particular, seu desempenho profissional, situação econômica, estado de saúde, preferências sexuais, confiabilidade ou comportamento.

Encarregado: prestador de serviços que, com caráter de pessoa física ou jurídica ou autoridade pública alheia à organização do Responsável, trata dados pessoais em nome e por conta deste.

Padrões: padrões de Proteção de Dados Pessoais para os Estados Ibero-americanos aprovados pela RIPD em 2017.

Exportador de dados: pessoa física ou jurídica de natureza privada, autoridade pública, serviços, órgão ou prestador de serviços localizado no território de um Estado que realize transferências internacionais de dados pessoais, de acordo com o disposto nos presentes Padrões.

Importador de dados: pessoa física ou jurídica de caráter privado, autoridade pública, serviços, órgão ou prestador de serviços localizado em um terceiro país que recebe dados pessoais de um Exportador de dados através de uma transferência internacional de dados pessoais.

Lei Aplicável: é a lei de proteção de dados pessoais da jurisdição do Exportador de dados.

Medidas administrativas, físicas e técnicas: medidas destinadas a prevenir danos, perdas, alterações, destruição, acesso e, em geral, qualquer uso ilícito ou não autorizado dos Dados pessoais, mesmo quando ocorra acidentalmente, suficientes para garantir a confidencialidade, integridade e disponibilidade dos Dados pessoais.

Responsável: quando um Encarregado do tratamento recorre a outro Encarregado para realizar certas atividades de tratamento por conta do Responsável.

Terceiros beneficiários: titular cujos dados pessoais são objeto de uma transferência internacional em virtude do presente Acordo. O Titular é um terceiro beneficiário dos direitos previstos a seu favor nas CCM e, portanto, pode exercer os direitos que as CCM reconhecem a ele, mesmo que o contrato modelo entre as partes não tenha sido assinado.

Titular: pessoa física a quem corresponde os dados pessoais.

Transferência ulterior: transferência de dados realizada pelo Importador de dados para um terceiro localizados fora da jurisdição do Exportador de dados que cumpre com as garantias estabelecidas nas CCM.

Tratamento: qualquer operação ou conjunto de operações realizadas por meio de procedimentos físicos ou automatizados realizados sobre dados pessoais, relacionados, incluindo, mas não limitando a obtenção, acesso, registro, organização, estruturação, adaptação, indexação, modificação, extração, consulta, armazenamento, conservação, elaboração, transferência, divulgação, posse, aproveitamento e, em geral, qualquer uso ou disposição de dados pessoais.

Violação da segurança dos dados pessoais: qualquer dano, perda, alteração, destruição, acesso e, em geral, qualquer uso ilícito ou não autorizado dos dados pessoais, mesmo que ocorra acidentalmente.

Cláusula 2: Efeitos e invariabilidade das cláusulas

2.1. Modificação das cláusulas do modelo: limites

O presente Acordo baseado em cláusulas contratuais modelo estabelece garantias adequadas ao Titular em relação às transferências de seus dados, de Responsável(eis) a Responsável(eis), desde que as Cláusulas não sejam modificadas em sua essência em relação ao modelo original, exceto para completar a capa e os anexos. Isso não impede que as Partes incluam as cláusulas contratuais modelo em um contrato mais amplo, nem que adicionem outras cláusulas ou garantias adicionais, desde que não contradigam, direta ou indiretamente, as presentes cláusulas contratuais modelo nem prejudiquem os direitos do Titular.

2.2 Hierarquia com a Lei Aplicável: interpretação

a. O presente Acordo deverá ser lido e interpretado de acordo com as disposições da Lei Aplicável.

b. As Partes poderão agregar novas definições de termos, salvaguardas e garantias adicionais nas presentes cláusulas modelo quando for necessário para cumprir com a Lei aplicável e desde que isso não suscite um detrimento às proteções outorgadas pelas cláusulas modelo.

c. O presente Acordo não poderá ser interpretado de forma a entrar em conflito com os direitos e obrigações estabelecidos na Lei aplicável.

d. O presente Acordo entende-se estar sem prejuízo das obrigações às quais o Exportador de dados está sujeito em virtude de sua legislação ou da Lei aplicável.

2.3. Hierarquia com outros acordos

Em caso de contradição entre este Acordo e as disposições dos acordos conexos entre as Partes, estabelece-se que as cláusulas do presente Acordo prevalecerão.

Cláusula 3: Terceiros beneficiários

Os Titulares poderão invocar, como Terceiros beneficiários, as cláusulas do presente Acordo contra o Exportador de Dados e/ou o Importador de dados e exigir deles o seu cumprimento.

Cláusula 4: Descrição da transferência ou transferências, e seus propósitos

Os detalhes e características da transferência ou transferências e, em particular, as categorias de Dados pessoais que são transferidos e os propósitos para os quais são transferidos estão detalhados no Anexo B do presente Acordo.

Cláusula 5: Cláusula de incorporação

Os Titulares poderão invocar, como Terceiros beneficiários, as cláusulas do presente Acordo contra o Exportador de Dados e/ou o Importador de dados e exigir deles o seu cumprimento.

Os detalhes e características da transferência ou transferências e, em particular, as categorias de Dados pessoais que são transferidos e os propósitos para os quais são transferidos estão detalhados no Anexo B do presente Acordo.

a. As Partes concordam que qualquer entidade que não faça parte do presente Acordo poderá, com o prévio consentimento de todas as Partes intervenientes, aderir-se a este Acordo a qualquer momento, seja como Exportador de dados ou como Importador de dados, assinando o modelo do Anexo A, e completando os outros Anexos, se for o caso.

b. Quando tiver assinado o Anexo A e tiver concluído os outros anexos, quando aplicável, a entidade aderente será considerada Parte do presente Acordo e terá os direitos e obrigações de um Exportador de dados ou um Importador de dados, dependendo da categoria em que tenha se aderido ao Acordo conforme o estabelecido no Anexo A.

c. A entidade que aderir ao Acordo não adquirirá direitos e obrigações nos termos deste Acordo decorrentes do período anterior à sua adesão.

Segunda parte: obrigações das partes

Cláusula 6: Garantias em termos de proteção de dados

6.1 Princípio de responsabilidade

a. O Exportador de dados garante que tem feito esforços razoáveis para determinar que o Importador de dados poderá, aplicando as Medidas administrativas, físicas e técnicas adequadas, cumprir com suas obrigações atribuídas nos termos do presente Acordo.

b. O Importador de dados implementará os mecanismos necessários para comprovar o cumprimento dos princípios e obrigações estabelecidas

no presente Acordo, bem como prestará contas sobre o tratamento de Dados pessoais sob sua posse ao Titular e à Autoridade controle competente.

c. O Importador de dados revisará e avaliará permanentemente os mecanismos que adota voluntariamente para esse fim para cumprir com o princípio da responsabilidade, com o intuito de mensurar seu nível de eficácia em termos de cumprimento deste Contrato.

6.2. Princípio de finalidade

a. O Importador de dados não poderá tratar os Dados pessoais objeto deste Acordo para fins diferentes daqueles indicados no Anexo B.

b. Somente poderá tratar os Dados pessoais com outros fins: *i)* quando tiver obtido o consentimento prévio do Titular; *ii)* quando necessário para o estabelecimento, exercício ou a defesa de reclamações no âmbito de procedimentos administrativos, regulatórios ou judiciais específicos; *iii)* quando o tratamento for necessário para proteger os interesses vitais do Titular ou de outra pessoa física.

6.3. Transparência

a. Como objetivo de que os Titulares possam exercer eficazmente os direitos outorgados a eles por este Acordo, o Importador de dados irá informá-los, diretamente ou através do Exportador de dados: *i)* sobre sua identidade e dados de contato; *ii)* as categorias de Dados pessoais processados e seus propósitos; *iii)* o direito de solicitar uma cópia do presente Acordo gratuitamente; *iv)* quando tiver a pretensão de fazer Transferências ulteriores dos Dados pessoais para terceiros, do destinatário ou das categorias de destinatários e sua finalidade.

b. O disposto não será de aplicação quando o Titular já dispuser da informação ou quando a comunicação de tal informação for impossível ou envolva um esforço desproporcional para o Importador de dados.

c. Caso seja solicitada uma cópia do Acordo, as Partes poderão excluir aquelas seções ou anexos do Acordo que contenham segredos comerciais ou outras informações confidenciais, tais como Dados pessoais de terceiros ou informações reservadas em termos dos regulamentos das Partes.

6.4 Precisão e minimização de dados

a. As Partes devem garantir que os Dados pessoais sejam precisos e, se necessário, que estejam atualizados. O Importador de dados tomará todas as medidas necessárias para que os Dados pessoais imprecisos em relação aos propósitos para os quais são tratados sejam excluídos ou ratificados sem dilação.

b. Se uma das Partes tomar conhecimento de que os Dados pessoais que transferiu ou recebeu são imprecisos ou obsoletos, informará sobre isso a outra parte sem dilação indevida.

c. O Importador de dados se assegurará que os Dados pessoais sejam adequados, relevantes e limitados ao necessário em relação aos propósitos do tratamento.

6.5. Limitação do prazo de conservação

a. O Importador de dados não conservará os Dados pessoais por mais tempo do que o necessário para os fins cujo são tratados.

b. O Importador de dados estabelecerá medidas administrativas, físicas e técnicas adequadas para garantir o cumprimento dessa obrigação, tais como a supressão ou Anonimização dos dados e de todas as cópias de backup ao finalizar o período de conservação.

6.6 Princípio de segurança

a. O Importador de dados e, durante a transferência, também o Exportador de dados estabelecerão e manterão Medidas de caráter administrativo, físico e técnico suficientes para garantir a confidencialidade, integridade e disponibilidade dos Dados pessoais objeto deste Acordo.

Para a determinação das medidas de segurança, o Importador de dados considerará os seguintes fatores:

i) O risco aos direitos e liberdades dos Titulares, em particular, pelo potencial valor quantitativo e qualitativo que os dados pessoais tratados podem ter para um terceiro não autorizado para sua posse.

ii) O estado da técnica.

iii) Os custos de aplicação.

iv) A natureza dos Dados Pessoais tratados, especialmente se forem Dados pessoais sensíveis.

v) O escopo, o contexto e os propósitos do tratamento.

vi) As possíveis consequências que se derivariam de uma violação para os titulares.

vii) As violações prévias ocorridas no tratamento de Dados pessoais.

b. As partes concordaram com as Medidas administrativas, físicas e técnicas estabelecidas no Anexo C do presente Acordo de Dados pessoais objeto da transferência internacional.

c. O Importador de dados realizará controles periódicos para garantir que essas medidas continuem a fornecer um nível adequado de segurança.

6.6.1 Violação à segurança dos dados pessoais

a. No caso de Violação da segurança dos dados pessoais tratados pelo Importador de dados no âmbito do presente Acordo, o Importador de dados tomará as medidas adequadas para resolvê-los e mitigar os possíveis efeitos negativos.

b. O Importador de dados documentará todos os fatos relevantes relativos à violação da segurança dos dados pessoais, como seus efeitos e as medidas corretivas tomadas, e manterá um registro delas.

c. Quando alguma das Partes tomar conhecimento de uma Violação de segurança de dados, notificará a outra Parte, a Autoridade de controle competente e os Titulares afetados de tal evento, sem dilação alguma e no máximo dentro de um período não superior a cinco (5) dias.

d. A notificação que seja realizada em virtude do parágrafo anterior será redigida em linguagem clara e simples. Essa notificação deve conter, pelo menos, as seguintes informações:

i) A natureza do incidente.

ii) Os Dados pessoais comprometidos.

iii) As ações corretivas tomadas imediatamente.

iv) No caso de notificação ao Titular, as recomendações aos mesmos sobre as medidas que este último pode adotar para proteger seus interesses.

v) Os meios disponíveis ao Titular para obter mais informações a respeito.

e. Na medida em que o Importador de dados não possa fornecer todas as informações ao mesmo tempo, poderá fazê-lo em fases sem mais dilações indevidas.

f. A notificação aos Titulares não será necessária quando tal notificação envolver um esforço desproporcional. Neste caso, o Importador de dados fará uma comunicação pública ou adotará uma medida semelhante para informar o público sobre a Violação de segurança de dados.

6.7 Tratamento sob a autoridade do Importador de dados e princípio de confidencialidade

a. O Importador de dados irá garantir que as pessoas que atuem sob sua autoridade tratem apenas os dados seguindo as instruções do Importador de dados, e estabelecerá controles ou mecanismos para que os que intervenham em qualquer estágio do tratamento dos dados pessoais mantenham e respeitem a confidencialidade deles, obrigação que subsistirá mesmo após o término de suas relações com o Exportador de dados.

b. O Importador de dados irá garantir que as pessoas autorizadas a tratar os Dados pessoais tenham se comprometido a respeitar a confidencialidade ou estejam sujeitas a uma obrigação legal de confidencialidade.

6.8. Tratamento de Dados pessoais sensíveis

a. Na medida em que a transferência inclua Dados pessoais sensíveis, o Importador de dados aplicará restrições específicas e garantias adicionais adaptadas à natureza específica dos dados e ao risco especial de que se trate.

b. Essas medidas podem consistir em, por exemplo, na redução de pessoal autorizado a acessar os Dados pessoais, acordos especiais de confidencialidade, medidas adicionais de segurança (como a Anonimização) e/ou restrições adicionais em relação à comunicação ulterior.

c. Na medida em que a transferência inclua Dados pessoais relativos a crianças e adolescentes, as Partes devem priorizar a proteção do interesse superior destes, de acordo com a Convenção sobre os Direitos da Criança e outros instrumentos internacionais.

6.9. Transferências ulteriores

a. O Importador de dados somente poderá comunicar os Dados pessoais a terceiros localizados fora da jurisdição do Exportador de dados se o terceiro

estiver vinculado pelo presente Acordo ou concorda em submeter-se a ele. Caso contrário, o Importador de dados só poderá fazer uma Transferência ulterior se:

> i) Para o caso em que a Lei Aplicável assim o dispuser, esta transferência ulterior irá direcionada a um país que tenha sido objeto de uma declaração de adequação de seu nível de proteção de dados pessoais de acordo com as disposições da Lei Aplicável, desde que tal declaração abranja a Transferência ulterior;
>
> ii) o terceiro destinatário da Transferência ulterior fornece de algum modo garantias adequadas, de acordo com as disposições da lei aplicável, no que diz respeito aos Dados pessoais sujeitos à Transferência ulterior;
>
> iii) o terceiro subscreve um instrumento vinculativo com o Importador de dados que garanta o mesmo nível de proteção de dados que o presente Acordo, e o Importador de dados entrega uma cópia dessas garantias ao Exportador de dados;
>
> iv) a Transferência ulterior é necessária para a formulação, exercício ou defesa de queixas e reclamações no âmbito de procedimentos administrativos, regulatórios ou judiciais específicos;
>
> v) se for necessário para proteger os interesses vitais do Titular ou de outra pessoa física; ou
>
> vi) se as demais condições não forem atendidas, o Importador de dados obteve o Consentimento expresso do Titular para uma Transferência ulterior em uma situação específica, após ter informado a sua finalidade, a identidade do destinatário e os possíveis riscos de tal transferência para o Titular devido à falta de garantias adequadas em termos de proteção de dados. Neste caso, o Importador de dados informará ao Exportador de dados e, a pedido deste, e enviará uma cópia da informação fornecida ao Titular.

b. Qualquer transferência ulterior estará sujeita a que o Importador de dados, adote as demais garantias previstas neste Acordo e, em particular, cumpra com o princípio da finalidade.

6.10. Documentação e cumprimento

a. As partes deverão poder demonstrar o cumprimento das obrigações derivadas do presente Acordo.

b. Em particular, o Importador de dados manterá documentação suficiente das atividades de tratamento realizadas sob sua responsabilidade, que colocará à disposição do Exportador de Dados e, se for caso, à disposição da Autoridade de controle competente mediante prévia solicitação.

Cláusula 7: Direitos do Titular

a. O Importador de dados, se for o caso, com o auxílio do Exportador de dados, tramitará, gratuitamente e sem dilação indevida e no máximo dentro de um prazo de quinze dias úteis, a menos que as normas aplicáveis indiquem um tempo menor, a partir do recebimento da consulta ou solicitação, as consultas e solicitações recebidas de Titulares em relação ao tratamento de seus Dados pessoais e o exercício dos direitos que lhes outorga o presente Acordo.

b. O Importador de dados tomará as medidas adequadas para facilitar tais consultas e solicitações e o exercício dos direitos dos Titulares. Todas as informações fornecidas aos Titulares devem ser inteligíveis e de fácil acesso, com linguagem clara e simples.

c. Em particular, o Titular terá o direito de:

i) solicitar a confirmação da existência do tratamento de seus Dados pessoais, acessar seus Dados pessoais que estejam em posse do Importador de dados, incluindo uma cópia completa destes, bem como conhecer quaisquer informações relacionadas com as condições gerais e específicas de seu tratamento, incluindo, entre outras informações, sobre as categorias de dados processados, a finalidade do tratamento, o período de retenção dos dados (ou o critério para determiná-lo), as Transferências ulteriores, incluindo os destinatários e a finalidade das mesmas, e informação sobre o direito de apresentar uma reclamação perante a Autoridade de controle competente;

ii) obter do Importador de dados a retificação ou correção de seus Dados pessoais, quando os mesmos se mostrem imprecisos, incompletos ou não atualizados;

iii) solicitar o cancelamento ou exclusão de seus Dados pessoais dos arquivos, registros e sistemas do Importador de dados, com o intuito de que os mesmos não estejam mais em sua posse e deixem de ser tratados por este último, quando os dados tiverem sido tratados em contravenção dos direitos de terceiros beneficiários decorrentes deste Acordo, ou se o Titular retirar o consentimento em que o tratamento se baseia;

iv) opor-se ao tratamento de seus Dados pessoais quando o tratamento visar o marketing direto, incluindo a elaboração de perfis, na medida em que esteja relacionada a tal atividade.

v) solicitar e acessar o Acordo assinado entre o Importador de Dados e o Exportador de Dados, eliminando a informação confidencial de terceiros alheios e reservada de acordo com as normas do Importador de Dados.

7.1 Limitações no exercício de direitos

a. O Importador de dados poderá denegar a solicitação de um Titular quando isso for permitido pela lei do país de destino e seja necessário e proporcional em uma sociedade democrática para salvaguardar objetivos importantes de interesse público em geral ou os direitos e liberdades dos indivíduos.

b. Se o Importador de dados pretende denegar a solicitação de um Titular, ele irá informá-lo sobre os motivos da denegação e da possibilidade de ajuizar uma reclamação junto à Autoridade controle competente ou de ajuizar uma ação judicial.

7.2 Direito de não ser objeto de decisões individuais automatizadas

a. O Importador de dados não tomará uma Decisão individual automatizada em relação aos Dados pessoais transferidos.

b. As disposições do parágrafo anterior não serão aplicáveis quando (i) esteja autorizado pela lei do país do Importador de dados que garanta medidas adequadas para a salvaguarda dos direitos do Titular, ou (ii) se baseie no consentimento demonstrável do Titular.

c. O responsável não pode realizar o tratamento automatizado de dados pessoais que tenha como efeito a discriminação dos titulares com base em sua origem racial ou étnica; crenças ou convicções religiosas, filosóficas e morais;

afiliação sindical; opiniões políticas; dados relacionados à saúde, à vida, preferência sexual ou orientação, bem como dados genéticos ou biométricos.

Cláusula 8. Reclamações

a. O Importador de dados informará aos Titulares, de forma transparente e em um formato de fácil acesso, através de notificação individual ou em seu site, o ponto de contato autorizado a processar as queixas e reclamações. Este irá processar as reclamações que receba dos Titulares o mais rápido possível. [OPÇÃO: O Importador de dados concorda que os Titulares também podem apresentar uma reclamação perante um órgão independente de resolução de litígios sem nenhum custo para o Titular. O Importador de dados informará aos Titulares, na forma estabelecida neste parágrafo, deste mecanismo de reparação e que eles não estão obrigados a recorrer a este nem a seguir uma sequência específica de vias de reparação.]

b. No caso de litígio entre um Titular e uma das Partes em relação ao cumprimento do presente Acordo, tal parte fará todos os esforços para resolver o problema amigavelmente em tempo hábil. As Partes devem se manter mutuamente informadas de tais litígios e, quando for o caso, irão cooperar de boa-fé para resolvê-los.

c. O Importador de dados compromete-se a aceitar e não controverter, quando o Titular invocar um direito de terceiro beneficiário decorrente deste Acordo, a decisão do Titular de:

i) apresentar uma reclamação à Autoridade de controle do Estado de sua residência habitual ou seu local de trabalho ou à Autoridade de controle competente;

ii) entrar com um processo judicial sobre seus Dados pessoais de acordo com as disposições da cláusula 14 deste Acordo.

d. O Importador de dados aceita cumprir quaisquer resoluções que sejam vinculantes às normas da Lei aplicável ou ao direito em questão.

Cláusula 9. Responsabilidade civil

a. Cada Parte será responsável perante a outra por qualquer dano ou prejuízo causado pela violação dos direitos e obrigações estabelecidos no presente Acordo.

b. Cada parte será responsável perante o Titular. O Titular terá o direito de ser indenizado por danos e prejuízos materiais ou imateriais que qualquer uma das Partes cause ao Titular por violar os direitos de terceiros beneficiários que derivem deste Acordo. Isso não prejudica a responsabilidade que a Lei aplicável atribui ao Exportador de dados.

c. Quando mais de uma parte for responsável por qualquer dano ou prejuízo causado ao Titular como resultado de uma violação do presente Acordo, todas as partes responsáveis serão solidariamente responsáveis.

d. As Partes acordam que, se uma das partes for considerada responsável nos termos do presente Acordo, estará legitimada para exigir à outra parte a indenização correspondente à sua responsabilidade pelo dano ou prejuízo.

Cláusula 10. Supervisão da Autoridade de controle competente

a. O Importador de dados concorda em submeter-se à jurisdição da Autoridade de controle competente e cooperar com ela em qualquer procedimento que vise garantir o cumprimento deste Acordo.

b. Em particular, o Importador de dados compromete-se a responder às solicitações, submeter-se a auditorias e cumprir as medidas tomadas pela Autoridade de controle e, em particular, as medidas corretivas e compensatórias. Enviará à Autoridade de controle por escrito a confirmação de que as providências cabíveis foram tomadas.

c. Da mesma forma, o Importador de dados concorda em submeter-se às faculdades da Autoridade de controle competente quanto à suspensão de transferências, suspensão de contratos e outras medidas correspondentes que esta julgar aplicáveis.

Cláusula 11. Direito e práticas do país que afetam o cumprimento das cláusulas

a. As partes confirmam que, no momento da celebração deste Acordo, realizaram esforços razoáveis para identificar se os dados transferidos estão cobertos por qualquer lei ou prática local da jurisdição do Importa-

dor de dados que vai além do que é necessário e proporcional em uma sociedade democrática para salvaguardar importantes objetivos de interesse público e pode razoavelmente esperar-se que afete as proteções, direitos e garantias concedidos sob este Acordo ao Titular. Com base no anterior, as partes confirmam que não estão cientes de que tal prática ou norma exista ou afete adversamente as proteções específicas previstas neste Acordo.

b. O Importador de dados compromete-se a notificar o Exportador de dados imediatamente se alguma dessas leis for aplicada a ele no futuro. De realizar tal notificação ou se o Exportador de dados tiver motivos para acreditar que o Importador de dados não pode mais cumprir com as obrigações deste Acordo, o Exportador de dados identificará as medidas apropriadas (por exemplo, medidas administrativas, físicas e técnicas para garantir a segurança) para remediar a situação.

c. Da mesma forma, poderá suspender as transferências objeto deste Acordo se considerar que as garantias adequadas não podem ser garantidas. Neste caso, o Exportador de dados terá o direito de rescindir este Acordo de acordo com as disposições da cláusula 12

d. Se um tribunal ou agência governamental exigir que o Importador de dados divulgue ou use os dados transferidos de forma que não esteja permitida por este Acordo, o Importador de dados revisará a legalidade de tal solicitação e a impugnará se, após uma minuciosa avaliação legal, concluir que existem razões razoáveis para considerar que a solicitação é ilegal de acordo com a legislação local e afeta os direitos garantidos por este Acordo. Na medida em que isso for permitido pela lei local, deverá também informar imediatamente ao Exportador de dados sobre o recebimento de tal solicitação. Se o Importador de dados estiver proibido de notificar o Exportador de dados de acordo com a Lei local, fará todos os esforços possíveis para obter uma isenção da proibição.

Terceira parte: disposições finais

Cláusula 12: Descumprimento das cláusulas e resolução do contrato

a. O Importador de dados informará imediatamente ao Exportador de dados caso não possa cumprir com alguma das cláusulas deste Acordo por qualquer motivo.

b. Se o Importador de dados não cumprir com as obrigações que lhe são impostas pelo presente Acordo, o Exportador de dados suspenderá a transferência de Dados pessoais para o Importador de dados até que o cumprimento seja novamente garantido ou o contrato seja rescindido.

c. O Exportador de dados terá o poder de rescindir este Acordo quando:

i) o Exportador de dados tenha suspendido a transferência de Dados pessoais para o Importador de dados nos termos do parágrafo anterior e não seja dado novamente cumprimento ao presente Acordo dentro de um prazo razoável e, em qualquer caso, no prazo de trinta (30) dias úteis contados a partir da suspensão;

ii) o Importador de dados viole de forma substancial ou persistentemente este Acordo; ou

iii) o Importador de dados não cumpra com uma resolução vinculante de um órgão jurisdicional ou Autoridade de controle competente em relação às obrigações atribuídas a ele nos termos deste Acordo. Neste caso, informará a Autoridade de controle competente sobre seu descumprimento.

d. Os Dados pessoais que tenham sido transferidos antes da resolução do contrato deverão, por escolha do Exportador de dados, ser devolvidos imediatamente ao Exportador de dados ou destruídos em sua totalidade. O mesmo se aplica às cópias dos dados. O Importador de dados deverá comprovar a destruição dos dados ao Exportador de dados. Até que os dados sejam destruídos ou devolvidos, o Importador de dados continuará a garantir o cumprimento com o presente Acordo. Se a lei do país aplicável ao Importador de dados proibir a devolução ou a destruição dos Dados Pessoais transferidos, o Importador de dados compromete-se a continuar garantindo o cumprimento do presente Acordo e só tratará os dados na medida e durante o período exigidos pelo direito do país.

Cláusula 13: Direito aplicável

O presente Acordo será regido pela Lei aplicável.

Cláusula 14: Escolha do fórum e jurisdição

a. Qualquer controvérsia decorrente deste presente Acordo será resolvida judicialmente nos tribunais de jurisdição do Exportador de dados.

b. Os Titulares também podem tomar medidas legais contra o Exportador de dados e/ou o Importador de dados, que poderão ser iniciadas, por escolha do Titular, no país do Exportador de dados, ou no qual o Titular residir. Com relação ao Importador de dados, eles poderão também tomar medidas legais no país do Importador de dados.

c. As Partes concordam em submeter-se à jurisdição prevista nesta cláusula.

Segunda parte: obrigações das partes

Cláusula 6: Garantias em termos de proteção de dados

6.1 Instruções

O Importador de dados realizará as atividades de tratamento dos Dados pessoais sem ostentar qualquer poder de decisão sobre o escopo e conteúdo dele, bem como limitará suas ações aos termos e instruções estabelecidos pelo Exportador de dados.

6.2 Princípio de responsabilidade

a. O Exportador de dados garante que tem feito esforços razoáveis para determinar que o Importador de dados poderá, aplicando as Medidas administrativas, físicas e técnicas adequadas, cumprir com suas obrigações atribuídas nos termos do presente Acordo.

b. O Importador de dados implementará os mecanismos necessários para comprovar o cumprimento dos princípios e obrigações estabelecidas no presente Acordo, bem como prestará contas sobre o tratamento de Dados pessoais sob sua posse ao Titular e à Autoridade controle competente.

c. O Importador de dados revisará e avaliará permanentemente os mecanismos que adota voluntariamente para esse fim para cumprir com o princípio da responsabilidade, com o intuito de mensurar seu nível de eficácia em termos de cumprimento deste Contrato.

6.3. Princípio de finalidade

O Importador de dados não poderá tratar os Dados pessoais objeto deste Acordo para fins diferentes dos indicados no Anexo B, exceto quando seguir instruções adicionais do Exportador de dados.

6.4. Transparência

a. Mediante solicitação prévia, as Partes disponibilizarão gratuitamente ao Titular uma cópia deste Acordo. De qualquer forma, o Importador de dados assume a responsabilidade de informar sobre sua existência. Podem ser excluídas seções ou anexos do Acordo que tenham segredos comerciais ou outras informações de tipo confidenciais, tais como Dados pessoais de terceiros ou informação reservada em termos dos regulamentos aplicáveis às Partes.

b. A presente cláusula entende-se sem prejuízo das obrigações atribuídas ao Exportador de dados pela legislação aplicável.

6.5 Precisão e minimização de dados

a. Se o Importador de dados tomar conhecimento de que os Dados pessoais que tenha recebido são imprecisos ou se tornaram obsoletos, informará sobre isso ao Exportador de dados sem dilação indevida.

b. Neste caso, o Importador de dados colaborará com o Exportador de dados para excluir ou retificar os dados.

6.6 Princípio de segurança

a) O Importador de dados e, durante a transferência, também o Exportador de dados estabelecerão e manterão Medidas de caráter administrativo, físico e técnico suficientes para garantir a confidencialidade, integridade e disponibilidade dos Dados pessoais objeto deste Acordo; em particular, a proteção contra a Violação da segurança dos dados pessoais. No momento de determinar um nível adequado de segurança, as partes deverão levar em consideração o estado da técnica, os custos de implementação, a natureza, o escopo, o contexto e os propósitos do tratamento e os riscos decorrentes do tratamento aos Titulares. Ao cumprir com as obrigações impostas no presente parágrafo, o Importador de dados aplicará, pelo menos, as Medidas administrativas, físicas e técnicas previstas no Anexo C deste Acordo. O Importador de dados realizará controles periódicos para garantir que essas medidas continuem a fornecer um nível adequado de segurança.

b) No caso de Violação da segurança de dados pessoais tratados pelo Importador de dados em virtude do presente Acordo, o Importador de dados tomará as medidas adequadas para resolvê-lo e, em particular, medidas para mitigar os efeitos negativos.

c) O Importador de dados também notificará o Exportador de dados dentro do prazo de setenta e duas (72) horas, assim que tiver conhecimento da Violação de segurança. Tal notificação incluirá uma descrição da natureza da Violação (na qual figurem, quando possível, as categorias e o número aproximado de Titulares e registros de Dados pessoais afetados), as consequências prováveis e as providências tomadas ou propostas para remediar a Violação da segurança e, em particular, se for o caso, medidas para mitigar seus possíveis efeitos negativos.

d) Quando e na medida em que todas as informações não possam ser fornecidas ao mesmo tempo, a notificação inicial fornecerá a informação disponível nesse momento e, à medida que coletadas, a informação adicional irá sendo fornecida sem dilação indevida.

e) O Importador de dados cooperará com o Exportador de dados e o auxiliará no cumprimento das obrigações atribuídas a ele pela Lei aplicável, especialmente no que diz respeito à notificação à Autoridade de controle competente e aos Titulares afetados, levando em consideração a natureza do tratamento e a informação disposta pelo Importador de Dados.

6.7. Tratamento sob a autoridade do Importador de dados e princípio de confidencialidade

a. O Importador de dados irá garantir que as pessoas que atuem sob sua autoridade somente tratarão os dados seguindo suas instruções, e apenas concederá acesso aos Dados pessoais aos membros de sua equipe na medida estritamente necessária para a execução, gestão e monitoramento do Acordo.

b. O Importador de dados assegurará que as pessoas autorizadas para tratar os Dados pessoais mantenham e respeitem a confidencialidade deles, obrigação que subsistirá mesmo após o término de suas relações com o Exportador de dados.

6.8. Tratamento de Dados pessoais sensíveis

a. Na medida em que a transferência inclua Dados pessoais sensíveis, o Importador de dados aplicará as restrições específicas e/ou garantias adicionais descritas no Anexo C deste Acordo.

b. Na medida em que a transferência inclua Dados pessoais relativos a crianças e adolescentes, o Importador deverá privilegiar a proteção do interesse superior destes, de acordo com a Convenção sobre os Direitos da Criança e outros instrumentos internacionais.

6.9 Transferências ulteriores

a. O Importador de dados só comunicará os Dados pessoais a um terceiro seguindo instruções documentadas do Exportador de dados.

b. Por outro lado, os dados só podem ser comunicados a terceiros localizados fora da jurisdição do Exportador se o terceiro estiver vinculado ao presente Acordo ou concordar em se submeter a este. Caso contrário, o Importador de dados somente poderá efetuar uma Transferência ulterior se:

> i) Para o caso em que a Lei Aplicável assim dispuser, esta transferência ulterior será direcionada a um país que tenha sido objeto de uma declaração de adequação de seu nível de proteção de dados pessoais de acordo com as disposições da Lei Aplicável, desde que tal declaração abranja a Transferência ulterior;

ii) o terceiro destinatário da Transferência ulterior fornece de certa forma garantias adequadas, de acordo com as disposições da Lei Aplicável, no que diz respeito aos Dados pessoais sujeitos à Transferência ulterior;

iii) a Transferência ulterior é necessária para a formulação, exercício ou defesa de reclamações no contexto de procedimentos administrativos, regulatórios ou judiciais específicos;

iv) se for necessário para proteger interesses vitais do Titular ou de outra pessoa física.

c. Qualquer transferência ulterior estará sujeita a que o Importador de dados adote as demais garantias previstas neste Acordo e, em particular, cumpra com o princípio da finalidade.

6.10 Documentação e cumprimento

a. As partes deverão poder demonstrar o cumprimento das obrigações derivadas do presente Acordo. Em particular, o Importador de dados conservará suficiente documentação das atividades de tratamento realizadas sob as instruções do Exportador, que serão disponibilizadas ao Exportador de dados e à Autoridade de controle competente sob prévia solicitação.

b. O Importador de dados responderá pronta e adequadamente às consultas do Exportador de dados relacionadas ao tratamento nos termos do presente Acordo.

c. O Importador de dados disponibilizará ao Exportador de dados todas as informações necessárias para demonstrar o cumprimento das obrigações previstas neste Acordo e, a pedido do Exportador de dados, permitirá e contribuirá para a realização de auditorias das atividades de tratamento abrangidas por este Acordo, em intervalos razoáveis ou se houver indícios de descumprimento. O Exportador de Dados pode optar por realizar a auditoria por si próprio ou autorizar um auditor independente. As auditorias poderão consistir em inspeções dos locais ou instalações físicas do importador de dados e, se for o caso, ser realizadas com aviso prévio.

d. As Partes colocarão à disposição da autoridade de controle competente, a pedido dela, as informações referidas nos parágrafos anteriores e, em particular, os resultados das auditorias.

6.11 Duração do tratamento e suspensão ou devolução dos dados

a. O tratamento por parte do Importador de dados só ocorrerá durante o período especificado no Anexo B deste Acordo.

b. Uma vez prestados os serviços de tratamento, o Importador de dados excluirá de forma segura, a pedido do Exportador de dados, todos os Dados pessoais tratados por conta do Exportador de dados e evidenciará isso ao Exportador de dados, ou devolverá ao Exportador de dados todos os dados e excluirá de forma segura as cópias existentes, se o Exportador de dados optar pela última opção. Até que os Dados pessoais sejam destruídos ou devolvidos, o Importador de dados continuará a garantir o cumprimento com o presente Acordo. Se o direito do país aplicável ao Importador de dados proibir a devolução ou destruição dos Dados pessoais, o Importador de dados se compromete a continuar garantindo o cumprimento do presente Acordo e somente tratará os dados na medida e durante o prazo exigido pelo direito do país do Importador de dados.

Cláusula 7: Recurso para sub encarregados

7.1. Forma de autorização do sub encarregado

[OPÇÃO 1: AUTORIZAÇÃO PRÉVIA ESPECÍFICA]:

a. O Importador de dados somente poderá subcontratar a um Sub encarregado as atividades de tratamento que realize por conta Exportador de dados em virtude do presente Acordo com a autorização prévia específica e por escrito do Exportador de dados. O Importador de dados apresentará a solicitação de autorização específica, pelo menos, no prazo de 15 dias úteis antes da contratação do Sub encarregado em causa, juntamente com a informação necessária para que o Exportador de dados possa dar resposta a solicitação. A lista de sub encarregados já autorizados pelo Exportador de dados figura no anexo D do presente Acordo. As Partes manterão o Anexo D atualizado.

[OPÇÃO 2: AUTORIZAÇÃO GERAL POR ESCRITO]:

a. O Importador de dados tem uma autorização geral do Exportador de dados para contratar sub encarregados que figurem em uma lista previamente acordada. O Importador de dados informará ao Exportador de dados especificamente e por escrito sobre as adições ou substituições de sub encarregados previstas nesta lista com pelo menos 15 dias úteis de antecedência, de modo que o Exportador de dados tenha tempo suficiente para formular uma objeção diante de tais alterações antes que o sub encarregado ou sub encarregados em questão sejam contratados. O Importador de dados fornecerá ao Exportador de dados a informação necessária para que este possa exercer seu direito de formular objeções.

7.2 Contrato com o sub encarregado

b. Quando o Importador de dados recorrer a um Sub encarregado para realizar atividades específicas de tratamento (por conta do Exportador de dados), fará isso por meio de um contrato escrito que estabeleça, em essência, as mesmas obrigações em matéria de proteção de dados que foram impostas ao Importador de dados em virtude do presente Acordo, especialmente no que diz respeito aos direitos dos Titulares, desde que sejam terceiros beneficiários. As partes concordam que, ao cumprir o presente Acordo, o Importador de dados também cumpre com as obrigações que lhe são atribuídas pela cláusula relativa às Transferências ulteriores. O Importador de dados também cumpre com as obrigações atribuídas a cláusula correspondente a Transferências ulteriores. O Importador de dados deve garantir que o sub encarregado cumpra com as obrigações a ele atribuídas no presente Acordo.

c. O Importador de dados fornecerá ao Exportador de dados, a pedido deste, uma cópia do contrato com o sub encarregado e de quaisquer alterações subsequentes do mesmo. Na medida em que for necessário para proteger informação confidencial, como Dados pessoais, o Importador de dados poderá proteger essa informação antes de compartilhar a cópia.

d. O Importador de dados seguirá sendo plenamente responsável ante o Exportador de dados pelo cumprimento das obrigações impostas ao Sub encarregado de seu contrato com o Importador de dados. O Importador de dados notificará o Exportador de dados os descumprimentos por parte do sub encarregado das obrigações atribuídas a ele em tal contrato.

Cláusula 8: Direitos dos Titulares

a. O Importador de dados notificará prontamente o Exportador de dados sobre as solicitações recebidas do Titular. Não responderá a tal solicitação por si só, a menos que o Exportador de dados o tenha autorizado a fazê-lo.

b. O Importador de dados auxiliará o Exportador de dados no cumprimento de suas obrigações, respondendo às solicitações de exercício de direitos que a Lei aplicável atribui aos Titulares. Nesse sentido, as Partes estabelecerão no Anexo C sobre medidas administrativas, físicas e técnicas adequadas, levando em consideração a natureza do tratamento, para garantir que será prestada a devida assistência ao Exportador na aplicação da presente cláusula, bem como o objeto e o escopo do auxílio necessário.

c. No cumprimento das obrigações atribuídas a ele nos dois parágrafos anteriores, o Importador de dados seguirá as instruções do Exportador de dados.

Cláusula 9: Reclamações

a. O Importador de dados informará aos Titulares, de forma transparente e em um formato de fácil acesso, através de notificação individual ou em seu site, o ponto de contato autorizado para registrar as queixas e reclamações. Este irá registrar as reclamações que receba dos Titulares o mais rápido possível. [OPÇÃO: O Importador de dados concorda que os Titulares também possam apresentar uma reclamação perante um órgão independente de resolução de litígios sem nenhum custo para o Titular. Informará aos Titulares, na forma estabelecida neste parágrafo, sobre este mecanismo de reparação e que eles não estão obrigados a recorrer a este nem a seguir uma sequência específica de vias de reparação.]

b. No caso de litígio entre um Titular e uma das Partes em relação ao cumprimento do presente Acordo, tal parte fará tudo que estiver no seu alcance para resolver o problema amigavelmente e em tempo hábil. As Partes se manterão mutuamente informadas de tais litígios e, quando for o caso, irão cooperar de boa-fé para resolvê-los.

c. O Importador de dados compromete-se a aceitar e não controverter, quando o Titular invocar um direito de Terceiro Beneficiário decorrente deste Acordo, a decisão do Titular de: (i) apresentar uma reclamação

à Autoridade de controle de dados do Estado de sua residência habitual ou seu local de trabalho ou à Autoridade de controle competente; (ii) instaurar uma ação legal sobre seus Dados pessoais.

d. O Importador de dados aceita acatar as resoluções vinculadas às normas da Lei aplicável ou o direito em questão.

Cláusula 10: Responsabilidade civil

a. Cada parte será responsável pela(s) outra(s) parte(s) por quaisquer danos e prejuízos causados a ele(s) por qualquer violação do presente Acordo.

b. O Importador de dados será responsável perante o Titular. O Titular terá o direito de ser indenizado por danos e prejuízos materiais ou imateriais que o Importador de Dados ou o Sub encarregado ocasionem ao Titular por violar os direitos de terceiros beneficiários decorrentes do presente Acordo. O acima exposto se entende sem prejuízo da responsabilidade do Exportador de dados nos termos da Lei aplicável.

c. As Partes concordam que, se o Exportador de dados for considerado responsável, de acordo com o parágrafo anterior, por danos ou prejuízos causados pelo Importador de dados (ou pelo sub encarregado), estará legitimado para exigir do Importador de dados a parte da indenização que seja de responsabilidade do Importador dos dados.

d. Quando mais de uma Parte for responsável por um dano ou prejuízo causado ao Titular como resultado de uma violação do presente Acordo, todas as Partes responsáveis serão solidariamente responsáveis.

e. As Partes concordam que, se uma parte for considerada responsável de acordo com os termos descritos no parágrafo anterior, estará legitimada para a exigir da outra Parte a indenização correspondente à sua responsabilidade pelo dano ou prejuízo.

f. O Importador de dados não pode alegar a conduta de um sub encarregado do tratamento para eludir sua própria responsabilidade.

Cláusula 11: Supervisão da Autoridade competente

a. O Importador de dados concorda em submeter-se à jurisdição da Autoridade de controle competente e a cooperar com ela em qualquer procedimento que vise garantir o cumprimento do presente Acordo.

b. Em particular, o Importador de dados compromete-se a responder às consultas, submeter-se a auditorias e cumprir com as medidas tomadas pela Autoridade de controle e, em particular, com as medidas corretivas e indenizatórias. Enviará à Autoridade de controle por escrito a confirmação de que as medidas necessárias foram tomadas.

Cláusula 12: Direito e práticas do país que afetam o cumprimento das cláusulas

a. As partes confirmam que, no momento de celebrar este Acordo, fizeram tudo que estava ao seu alcance para identificar se os dados transferidos estão cobertos por alguma lei ou prática local da jurisdição do Importador de dados que vai além do necessário e proporcional em uma sociedade democrática para salvaguardar importantes objetivos de interesse público e pode razoavelmente esperar-se que afete as proteções, direitos e garantias outorgadas sob este Acordo ao Titular. Baseado no exposto, as Partes confirmam que não estão cientes de que tal prática ou norma exista ou afete adversamente as proteções específicas previstas neste Acordo.

b. O Importador de dados compromete-se a notificar imediatamente o Exportador de dados se alguma dessas leis aplicar a ele no futuro. Se tal notificação for feita ou se o Exportador de dados tiver razões para acreditar que o Importador de dados não pode mais cumprir com as obrigações deste Acordo, o Exportador de dados identificará as medidas apropriadas (p. ex. medidas administrativas, físicas e técnicas para garantir a segurança) para remediar a situação. Da mesma forma, poderá suspender as transferências objeto deste Acordo se considerar que as garantias adequadas não podem ser asseguradas. Neste caso, o Exportador de dados terá o direito de rescindir este Acordo em conformidade com as disposições da cláusula 13.

c. Se um tribunal ou agência governamental solicitar que o Importador de dados divulgue ou use os dados transferidos de uma forma que de

outro modo não estaria permitida por este Acordo, o Importador de dados irá revisar a legalidade de tal solicitação e a impugnará se, após uma avaliação legal minuciosa, concluir que há motivos razoáveis para considerar que a solicitação é ilegal, de acordo com a legislação local e afeta os direitos garantidos por este Acordo. Na medida em que isso estiver permitido pela lei local, também deverá informar imediatamente ao Exportador de dados que recebeu tal solicitação. Se o Importador de dados estiver proibido de notificar o Exportador de dados de acordo com a lei local, fará tudo que estiver ao seu alcance para obter uma isenção da proibição.

Terceira parte: disposições finais

Cláusula 13: Descumprimento das cláusulas e resolução do contrato

a. O Importador de dados informará imediatamente ao Exportador de dados, caso ele não possa cumprir com alguma das cláusulas deste Acordo por qualquer motivo.

b. Caso o Importador de dados não cumpra com as obrigações atribuídas a ele pelo presente Acordo, o Exportador de dados suspenderá a transferência de dados pessoais ao Importador de dados até que o cumprimento seja novamente garantido ou o contrato seja rescindido.

c. O Exportador de dados terá o poder de rescindir este Acordo quando:

i) o Exportador de dados tenha suspendido a transferência de dados pessoais para o Importador de dados nos termos do parágrafo anterior e não volte a ser dado cumprimento ao presente Acordo dentro de um prazo razoável e, em qualquer caso, no prazo de 30 (trinta) dias úteis a contar da data da suspensão; ii) o Importador de dados viole substancial ou persistentemente o presente Acordo; ou iii) o Importador de dados não cumpra com uma resolução vinculante de um órgão jurisdicional ou Autoridade de controle competente em relação às suas obrigações atribuídas nos termos do presente Acordo. Neste caso, informará a Autoridade de controle competente sobre seu descumprimento.

d. Os dados pessoais que tenham sido transferidos antes da resolução do contrato deverão, por escolha do Exportador de dados, ser devol-

vidos imediatamente ao Exportador de dados ou ser destruídos em sua totalidade. O mesmo se aplica às cópias dos dados. O Importador de dados evidenciará a destruição dos dados ao Exportador de dados. Até que os dados sejam destruídos ou devolvidos, o Importador de Dados continuará a garantir o cumprimento com o presente Acordo. Se o direito do país aplicável ao Importador de dados proibir a devolução ou destruição dos Dados pessoais transferidos, o Importador de dados compromete-se a seguir garantindo o cumprimento deste Acordo e somente tratará os dados na medida e durante o prazo exigido pelo direito do país.

Cláusula 14: Direito aplicável

O presente Acordo será regido pela Lei aplicável.

Cláusula 15: Escolha do fórum e jurisdição

a. Qualquer controvérsia decorrente do presente Acordo será resolvida judicialmente nos tribunais da jurisdição do Exportador de dados.

b. Os Titulares também poderão tomar medidas legais contra o Exportador de dados e/ou o Importador de dados, as quais poderão ser iniciadas, por escolha do Titular, no país do Exportador de dados, ou no qual o Titular residir. Com relação ao Importador de dados, eles também poderão tomar medidas legais no país do Importador de dados.

c. As Partes concordam em submeter-se à jurisdição prevista nesta cláusula.

Anexo D – Norma Peruana

Deliberação da Direção nº 074-2022-JUS/DGTAIPD

Lima, 17 de outubro de 2022

O artigo 2, parágrafo 6, da Constituição Política do Peru afirma que os serviços de informática, informatizados ou não, públicos ou privados, não fornecem informações que afetem a privacidade pessoal ou familiar;

Que a Lei nº 29733, Lei de Proteção de Dados Pessoais, visa garantir o direito fundamental à proteção de dados pessoais, previsto no parágrafo 6 do artigo 2º da Constituição Política do Peru;

Que, a referida norma legal, criou a Autoridade Nacional de Proteção de Dados Pessoais como órgão competente para realizar as ações necessárias para o cumprimento do objeto e demais disposições da referida Lei nº 29733 e seu Regulamento aprovado pelo Decreto Supremo nº 003-2013-JUS;

A alínea h) do artigo 7º da Lei nº 29809, Lei da Organização e Funções do Ministério da Justiça e dos Direitos Humanos, estabelece que o Ministério da Justiça e dos Direitos Humanos, no âmbito das suas competências específicas, exerce a Autoridade Nacional de Proteção de Dados Pessoais;

Que o artigo 70º do Regulamento sobre a Organização e Funções do Ministério da Justiça e dos Direitos Humanos, aprovado pelo Decreto Supremo nº 013-2017-JUS, estabelece que compete à Direção-Geral da Transparência, Acesso à Informação Pública e Proteção de Dados Pessoais exercer a Autoridade Nacional de Proteção de Dados Pessoais;

Que, nos termos das alíneas c) e g) do artigo 71º do Regulamento de Organização e Funções do Ministério da Justiça e dos Direitos Humanos, a Direção-Geral da Transparência, Acesso à Informação Pública e Proteção de Dados Pessoais é competente para emitir as orientações necessárias ao cumprimento das normas, bem como para promover a cultura no âmbito da sua competência;

Que o parágrafo 10 do artigo 2º da Lei nº 29733 define o fluxo transfronteiriço de dados como a transferência internacional de dados pessoais para um destinatário localizado em um país diferente do país de origem dos dados, independentemente do meio em que se encontrem, do meio pelo qual a transferência foi realizada ou do tratamento que recebem;

Que o artigo 11 da Lei nº 29733 prevê como um de seus princípios norteadores o Nível Adequado de Proteção, que estabelece que, para o fluxo transfronteiriço de dados pessoais, deve ser garantido um nível de proteção suficiente para que os dados pessoais sejam tratados ou, pelo menos, comparável ao previsto nesta Lei ou em normas internacionais;

O artigo 2º, nº 12, da Lei nº 29733 define o Nível Suficiente de Proteção de Dados Pessoais, afirmando que é o nível de proteção que inclui, no mínimo, o registo e o respeito dos princípios orientadores da Lei, bem como medidas técnicas de segurança e confidencialidade adequadas à categoria de dados em causa;

Que, de acordo com o artigo 15º da Lei nº 29733, o titular e o subcontratante de dados pessoais devem realizar o fluxo transfronteiriço de dados apenas se o país destinatário mantiver níveis de proteção adequados em conformidade com esta lei;

O artigo 24 do Regulamento da Lei nº 29733 estabelece que os fluxos transfronteiriços de dados pessoais serão possíveis quando o destinatário ou importador dos dados pessoais assumir as mesmas obrigações que correspondem ao titular do banco de dados pessoais ou controlador de dados que, como emissor ou exportador, transferiu os dados pessoais. Para tanto, de acordo com o artigo 25 do mesmo órgão regulador, prevê que o emissor ou exportador poderá utilizar cláusulas contratuais ou outros instrumentos jurídicos que estabeleçam, pelo menos, as mesmas obrigações a que está sujeito, bem como as condições em que o titular consentiu com o tratamento de seus dados pessoais;

Que, de 2014 até hoje, o Peru, por meio da Autoridade Nacional de Proteção de Dados Pessoais, faz parte da Rede Ibero-Americana de Proteção de Dados (RIPD). Em 22 de outubro de 2021, foi realizada a XIX Reunião da Rede Ibero-Americana de Proteção de Dados, em cuja declaração final, os Estados ibero-americanos, bem como os empresários, foram instados a levar em consideração as Cláusulas Contratuais Modelo desenvolvidas pela RIPD para transferências internacionais, principalmente trans-

ferências para jurisdições inadequadas. Isso porque essas cláusulas são um meio de cumprir os princípios da proteção de dados pessoais e, por sua vez, uma alternativa economicamente viável para os empresários que não terão que negociar acordos individuais, mas aderirão a um conjunto de cláusulas previamente aprovadas pela Autoridade;

Que, após um período de recebimento de comentários e aprovação de uma versão final, em 27 de setembro de 2022, a Secretaria Permanente da RIPD publicou em seu site o Guia para a Implementação de Cláusulas Contratuais Modelo para a Transferência Internacional de Dados Pessoais e seus Anexos, a fim de estabelecer os principais aspectos a serem levados em consideração quando as transferências internacionais de dados pessoais são feitas por meio do uso de Cláusulas-padrão Contratual. Este guia apresenta diretrizes a serem consideradas por aqueles que devem fazer transferências internacionais de dados pessoais para jurisdições inadequadas dos países membros da RIPD;

Que o objetivo das Cláusulas Contratuais Modelo é garantir e facilitar o cumprimento dos requisitos previstos na lei de proteção de dados do país exportador de dados pessoais para a transferência desses dados para um terceiro país que não tenha sido reconhecido com um nível de proteção adequado, de modo que a proteção inicialmente concedida aos dados pessoais continue independentemente de onde esses dados estejam localizados;

Que, de acordo com o exposto, o uso de Cláusulas Contratuais Modelo pode ajudar a superar as limitações às transferências de dados decorrentes de diferenças no nível de proteção entre diferentes países, considerando que tais cláusulas contribuem para a construção da convergência no nível contratual, sem necessariamente exigir convergência no nível do país;

Que, a utilização de Cláusulas Contratuais Modelo permite que as empresas não tenham de negociar e acordar acordos em cada caso individual, com o custo econômico que isso implica (para representação legal e tempo), uma vez que a existência destas cláusulas permite confiança no modelo da Autoridade Nacional, que foi devidamente aprovado no ambiente RIPD, sabendo que, ao implementá-los e cumpri-los, as empresas e entidades cumprem com as suas obrigações legais relativas à transferência internacional de dados pessoais com uma solução simples e prática;

Que, de acordo com a seção Esclarecimentos e Limitações do Guia para a Implementação de Cláusulas Contratuais Modelo para a Trans-

ferência Internacional de Dados Pessoais, a aplicação e o uso das duas cláusulas contratuais modelo (Contrato Modelo sobre a Transferência Internacional de Dados Pessoais entre o Controlador e o Controlador e o Contrato Modelo sobre a Transferência Internacional de Dados Pessoais entre o Controlador e o Operador devem ser realizados em harmonia com as recomendações, resoluções e determinações das autoridades locais de proteção de dados pessoais e, sobretudo, com a legislação local aplicável;

Que, de acordo com o exposto, é conveniente aprovar as Cláusulas Contratuais Modelo para a Transferência Internacional de Dados Pessoais contidas nas Cláusulas Contratuais Modelo para o Guia de Implementação da Transferência Internacional de Dados Pessoais da RIPD, para fins de disponibilização ao público, no âmbito das disposições dos artigos 24 e 25 do Regulamento da Lei nº 29733;

Que, de acordo com o disposto na Constituição Política do Peru, Lei nº 29733, Lei de Proteção de Dados Pessoais, seu Regulamento aprovado pelo Decreto Supremo nº 003-2013-JUS, alíneas c) e g) do artigo 71 do Regulamento sobre Organização e Funções do Ministério da Justiça e Direitos Humanos, aprovado pelo Decreto Supremo nº 013-2017-JUS, e o Regulamento do Decreto Legislativo nº 1353 que cria a Autoridade Nacional para a Transparência e Acesso à Informação Pública, reforça o Regime de Proteção de Dados Pessoais e a regulamentação da gestão de interesses aprovada pelo Decreto Supremo nº 019-2017-JUS;

Resolução

PRIMEIRO. Aprovação

Aprovar as Cláusulas Contratuais Modelo para a Transferência Internacional de Dados Pessoais, cujo texto faz parte do Guia para a Implementação de Cláusulas Contratuais Modelo para a Transferência Internacional de Dados Pessoais da Rede Ibero-Americana de Proteção de Dados, que se inclui como anexo a esta Resolução da Diretoria.

SEGUNDO. Publicação

Esta Resolução Diretora e seu Anexo estão publicados no portal institucional do Ministério da Justiça e Direitos Humanos: www.gob.pe/minjus; e, no portal institucional da Autoridade Nacional de Proteção de Dados Pessoais: www.gob.pe/anpd.

TERCEIRO. Difusão

A Direção Geral de Transparência, Acesso à Informação Pública e Proteção de Dados Pessoais do Ministério da Justiça e Direitos Humanos é responsável pela divulgação desta Resolução da Diretoria e seu Anexo.

Inscreva-se e comunique-se.

Eduardo Luna Cervantes
Diretor Geral
Direção-Geral da Transparência, Acesso à
Informação Pública e Proteção de Dados Pessoais

Anexo E - Norma Uruguaia

Resolução nº 23/021

08/06/2021

Delibera-se sobre a necessidade de atualização da Resolução nº 4/019, de 12 de março de 2019, sobre os países ou organismos considerados aptos para transferências internacionais de dados, de acordo com o disposto no artigo 23 da Lei nº 18.331, de 11 de agosto de 2008.

Montevidéu, 8 de junho de 2021.

TENDO VISTO: A necessidade de atualização da Resolução nº 4/019, de 12 de março de 2019, sobre os países ou organizações consideradas aptas para transferências internacionais de dados, de acordo com o disposto no artigo 23 da Lei nº 18.331, de 11 de agosto de 2008.

RESULTANDO:

I. Que a resolução indicada no Aviso substituiu o nº 17/009, de 12 de junho de 2009, e estabeleceu os territórios apropriados e, consequentemente, apropriados para as transferências internacionais de dados.

II. Que para este efeito foram consideradas as avaliações realizadas pela Unidade, e os casos em que há proteção equivalente à do Uruguai, seja por pertencer a uma determinada região ou por causa da avaliação realizada por entidades especializadas na avaliação da conformidade da legislação nacional com os princípios e direitos relacionados à proteção de dados.

III. Que, com base no contexto acima mencionado, a Resolução nº 4/019 estabeleceu que os membros da União Europeia e do Espaço Econômico Europeu, o Principado de Andorra, a República da Argentina, o setor privado do Canadá, as organizações incluídas no quadro "Privacy Shield" dos Estados Unidos da América, Guernsey, Ilha de Man, Ilhas Faroé, Estado de Israel, Japão, Jersey, Nova Zelândia, Reino Unido da Grã-Bretanha e Irlanda do Norte e Confederação da Suíça. Tal não prejudica as limitações previstas nas correspondentes decisões de adequação emitidas pela Comissão Europeia.

CONSIDERANDO:

I. Que a transferência internacional de dados implique sua transmissão fora do território nacional e constitua uma transferência ou comunicação que tenha como finalidade realizar um tratamento em nome do responsável pelo banco de dados ou tratamento estabelecido em território uruguaio.

II. Que o artigo 23 da Lei nº 18.331 prevê a proibição de transferências internacionais de dados com países ou organizações internacionais que não ofereçam níveis adequados de proteção, de acordo com as normas do Direito Internacional ou Regional sobre a matéria, com exceções; e esta Unidade é o órgão responsável por estabelecer os países e agências que fornecem esses níveis de proteção.

III. Que, nesta consideração, a Unidade levou em consideração especialmente as Normas de Proteção de Dados Pessoais para Estados Ibero-americanos emitidas pela Rede Ibero-Americana de Proteção de Dados e o Regulamento Geral Europeu de Proteção de Dados nº 2016/679 do Parlamento Europeu e do Conselho.

IV. Que os países membros da União Europeia cumprem as normas internacionais por aplicação do referido Regulamento e, por outro lado, considera-se que os países terceiros ou organizações que tenham sido objeto de decisões de adequação do Parlamento Europeu e do Conselho têm um nível de proteção adequado, uma vez que a sua regulamentação está em consonância com a da referida norma internacional.

V. Que, no caso de países terceiros ou organizações considerados apropriados, todas as limitações ou exceções previstas na decisão correspondente a que se refere o considerando anterior serão entendidas como incluídas nesta Resolução.

VI. Que no que respeita à adequação das organizações incluídas no quadro do "Privacy Shield", existem elementos derivados da análise do tratamento de dados nos Estados Unidos da América que levaram à invalidação desse quadro em território europeu, que justificam a revisão da Resolução desta Unidade. Estes elementos resultam, nomeadamente, do Acórdão do Tribunal de Justiça da União Europeia de 16 de julho de 2020.

VII. Que, portanto, as transferências internacionais realizadas para os Estados Unidos da América devem ser justificadas mediante o consentimento das partes interessadas ou qualquer das exceções previstas no artigo 23 da Lei nº 18.331 e, quando for o caso, ter a autorização expressa desta Unidade.

Para tanto, será dada especial atenção à adoção de cláusulas contratuais adequadas, à localização dos processadores de dados nos Estados que adotaram regulamentos de proteção de dados e à adoção do esquema de autocertificação disponibilizado pela Federal Trade Commission, entre outros elementos.

VIII. Que é necessário conceder aos controladores e operadores de dados que apoiaram suas transferências dentro da estrutura indicada no Considerando VI um período de tempo para os ajustes necessários.

ATENÇÃO: Para o acima,

A UNIDADE REGULADORA E DE CONTROLE
DE DADOS PESSOAIS

RESOLVE:

1º Substituir a Resolução nº 4/019, de 12 de março de 2019, e estabelecer que todos os países que, na opinião desta Unidade, tenham padrões e meios de proteção adequados para garantir sua efetiva aplicação sejam considerados adequados e, portanto, apropriados para transferências internacionais de dados. Em particular, os membros da União Europeia e do Espaço Econômico Europeu, o Principado de Andorra, a República da Argentina, o setor privado do Canadá, Guernsey, a Ilha de Man, as Ilhas Faroé, o Estado de Israel, o Japão, Jersey, a Nova Zelândia, o Reino Unido da Grã-Bretanha e Irlanda do Norte e a Confederação da Suíça são considerados adequados.

2º A realização de transferências para os países indicados no parágrafo anterior estará sujeita, se aplicável, ao disposto no Considerando V desta Resolução.

3º Conceder aos controladores e operadores pelas bases ou tratamento que, a partir da data de vigência desta Resolução, tenham baseado suas transferências para os Estados Unidos da América no âmbito do "Privacy Shield", um prazo de seis meses para ajustar as condições das transferências realizadas, a partir da publicação desta resolução no Diário Oficial.

4º Será notificado, publicado no Diário Oficial e no site da Unidade, e devidamente arquivado.

ASSINADO: FELIPE ROTONDO TORNARÍA
CONSELHO EXECUTIVO
URCDP

Resolução nº 50/022

29/12/2022

Fica deliberada a publicação do "Guia para a Implementação de Cláusulas Contratuais Modelo para a Transferência Internacional de Dados Pessoais (TIPD)" pela Rede Ibero-Americana de Proteção de Dados (RIPD).

TENDO VISTO: A publicação do "Guia para a Implementação de Cláusulas Contratuais Modelo para a Transferência Internacional de Dados Pessoais (TIPD)" pela Rede Ibero-Americana de Proteção de Dados (RIPD).

RESULTANDO:

I. Que a RIPD, organização da qual esta Unidade faz parte, publicou o documento indicado no Aviso, que é composto por um guia explicativo e dois modelos de acordos para a transferência internacional de dados pessoais, um entre o controlador e o controlador e outro entre o controlador e o operador.

II. Que o RIPD aprovou as "Normas de Proteção de Dados para Estados Ibero-americanos", que se destinam, entre outros, a "facilitar o fluxo de dados pessoais entre os Estados Ibero-americanos e além de suas fronteiras, a fim de contribuir para o crescimento social e econômico da região" (Artigo 1.1.d).

III. Que na elaboração do guia e das cláusulas contratuais, foram levadas em consideração as normas acima mencionadas, que de acordo com o documento devem ser lidas em conjunto e integralmente, sem prejuízo das eventuais adaptações que venham a ser feitas em nível nacional.

CONSIDERANDO:

I. Que o artigo 23 da Lei nº 18.331, de 11 de agosto de 2008, estabelece a vedação transferência de dados pessoais para territórios inadequados, sem prejuízo das exceções nele previstas.

II. Que o parágrafo final do artigo indicado no considerando anterior estabelece que "a Unidade de Regulação e Controle de Proteção de Dados Pessoais pode autorizar uma transferência ou uma série de transferências de dados pessoais para um país terceiro que não garanta um nível de proteção adequado, quando o controlador de dados ofereça garantias suficientes quanto à proteção da vida privada, direitos e liberdades fundamentais das pessoas, bem como no que diz respeito ao exercício dos respectivos direitos. Essas garantias podem ser derivadas de cláusulas contratuais adequadas."

III. Que, por meio da Resolução nº 23/021, de 8 de junho de 2021, estabeleceu os países considerados aptos para transferências internacionais de dados, e pela Resolução nº 41/021, de 8 de setembro de 2021, recomendou aos controladores e operadores de dados que pretendam realizar transferências internacionais de dados no âmbito do artigo 23 da Lei nº 18.331, a adoção de cláusulas contratuais com conteúdo mínimo indicado no Anexo I da referida resolução.

IV. Que as cláusulas contratuais publicadas pelo RIPD fornecem as garantias exigidas pelo regulamento, sem prejuízo das necessárias adaptações às regulamentações nacionais em vigor, a menos que a disposição contratual forneça maiores garantias aos titulares dos dados.

ATENÇÃO: ao acima,

O Conselho Executivo da Unidade de Regulação e Controlo de Dados Pessoais

RESOLVE:

1. Indicar aos controladores e processadores de dados que, no âmbito das transferências internacionais de dados realizadas nos termos do artigo 23 da Lei nº 18.331, eles podem usar as cláusulas contratuais incluídas no "Guia para a Implementação de Cláusulas Contratuais Modelo para a Transferência Internacional de Dados Pessoais (TIPD)" que estão anexadas a esta Resolução como Anexo I, com as adaptações que considerem adequadas para a sua adaptação às regulamentações nacionais, exceto nos casos em que as cláusulas ofereçam maiores garantias aos titulares dos dados.

2. Indicar aos controladores e processadores de dados que a utilização das cláusulas referidas na resolução anterior não exclui a autorização prévia desta Unidade para a transferência ou transferências que se pretendem realizar, de acordo com o disposto no parágrafo final do artigo 23 da Lei nº 18.331.

3. PUBLICAR

Assinado: Felipe Rotondo Tornaría
Conselho Executivo
URCDP

Resolução nº 70/023

05/12/2023

Complementam o disposto nas Resoluções nº 23/021, de 8 de junho de 2021 e nº 63/023, de 22 de novembro de 2023.

TENDO EM VISTA: A relevância de complementar o disposto nas Resoluções nº 23/021, de 8 de junho de 2021, e nº 63/023, de 22 de novembro de 2023.

RESULTANDO:

I. Que as referidas resoluções estabeleceram a lista de países e organizações aptas a realizar transferências internacionais de acordo com o disposto no artigo 23 da Lei nº 18.331, de 11 de agosto de 2008.

II. Que, de acordo com o disposto no art. 6º da Lei nº 18.331, a criação de bases de dados será lícita quando devidamente registradas, o que deverá ser feito no Registro de Bases de Dados criado pelo art. 1º do Decreto nº 664/008, de 22 de dezembro de 2008, na forma nele estabelecida e pelo art. 16 do Decreto nº 414/009, de 31 de agosto de 2009, alterado pelo artigo 1º do Decreto nº 308/014, de 22 de outubro de 2014.

III. Que, de acordo com o disposto no artigo 4º do Decreto nº 664/008, a Unidade de Regulação e Controle de Dados Pessoais está habilitada a acrescentar os elementos que entender necessários no âmbito do Registo de Bases de Dados, exigindo atualmente a indicação do destino da transferência internacional, independentemente do fundamento de legitimidade para tal transferência.

IV. O artigo 13 da Lei nº 18.331, conforme alterada pelo artigo 62 da Lei nº 20.075, de 20 de outubro de 2022, estabelece as informações que devem ser prestadas aos titulares antes da coleta de seus dados ou mediante sua solicitação, incluindo a existência ou não de transferências internacionais (parágrafo F). Este artigo também autoriza esta Unidade a estabelecer condições específicas para a publicação permanente das informações indicadas.

CONSIDERANDO:

I. Que, a partir dos regulamentos acima mencionados, decorre que antes da realização de transferências internacionais de dados, tanto para países ou organizações apropriadas quanto inadequadas, é necessário o registro prévio do banco de dados correspondente no Registro de Bancos de

Dados Pessoais realizado por esta Unidade. No caso de transferências para países ou territórios inadequados, também será exigida a verificação de uma das hipóteses previstas no artigo 23 da Lei nº 18.331, ou autorização prévia do Conselho Executivo da Unidade.

II. Que as decisões de adequação consideradas nas Resoluções indicadas no Aviso estabeleçam exceções ou aspectos especiais que devem ser considerados na avaliação da realização de uma transferência internacional, que é de responsabilidade dos controladores de dados de acordo com o disposto no artigo 12 da Lei nº 18.331, conforme alterada pelo artigo 39 da Lei nº 19.670, de 15 de outubro de 2018.

III. Que, no que diz respeito às transferências para as organizações a que se refere a Resolução nº 63/023, a especificidade do regime do Marco de Privacidade UE-EUA determina a necessidade de adotar salvaguardas adicionais para fins de sua aplicação às transferências realizadas a partir do Uruguai.

IV. Que a nova redação do artigo 13 da Lei nº 18.331 exige maior transparência na prestação de informações aos titulares, especialmente mencionando a transferência internacional de dados.

ATENÇÃO: Para o acima,

A UNIDADE REGULADORA E DE CONTROLE DE DADOS PESSOAIS RESOLVE:

1º Os controladores e operadores de dados que realizam transferências internacionais devem notificar os titulares dos dados, nas circunstâncias previstas no artigo 13 da Lei nº 18.331, de 11 de agosto de 2008 (conforme alterada pelo artigo 62 da Lei nº 20.075, de 20 de outubro de 2022), o destino dos seus dados, a função do importador, o prazo da transferência, a base de legitimação e as operações de tratamento realizadas pelo importador.

2º Os responsáveis terão um prazo de 6 (seis) meses para adaptar suas políticas de privacidade ao indicado na resolução anterior.

3º Reafirmar que o registro do banco de dados correspondente no Registro de Bancos de Dados Pessoais realizado por esta Unidade é um pré-requisito para qualquer operação de tratamento, incluindo a execução e eventual autorização de transferências internacionais.

Seção 4. Os controladores e as pessoas que pretendam realizar transferências internacionais para organizações incluídas no Quadro de Privacidade UE-EUA devem apresentar a esta Unidade, no momento do registro

do Banco de Dados ou antes da transferência, uma declaração expressa na qual a respectiva organização importadora declara que estendeu a aplicação das salvaguardas do referido marco aos dados transferidos do Uruguai. Caso tal declaração não seja feita, a transferência para as organizações acima mencionadas poderá ser feita por força de cláusulas contratuais apresentadas pelos gerentes, previamente autorizadas por esta Unidade, ou outros motivos previstos em lei.

5º Ser publicado e arquivado em tempo hábil.

Assinado por: Felipe Rotondo
Conselho Executivo
URCDP

Anexo F – Norma Argentina

AGÊNCIA ARGENTINA DE ACESSO À INFORMAÇÃO PÚBLICA

Resolução 198/2023

RESOL-2023-198-APN-AAIP

Cidade de Buenos Aires, 13/10/2023

TENDO VISTO Arquivo nº EX-2023-60881292- -APN-AAIP; as Leis nº 25.326, nº 27.275, nº 27.483 e nº 27.699; Decretos nº 1558 de 29 de novembro de 2001, nº 206 de 27 de março de 2017, nº 746 de 25 de setembro de 2017 e nº 899 de 3 de novembro de 2017; Resolução da AGÊNCIA DE ACESSO À INFORMAÇÃO PÚBLICA Nº 34 de 26 de fevereiro de 2019; a Disponibilização da Direção Nacional de Proteção de Dados Pessoais nº 60 de 16 de novembro de 2016; e

CONSIDERANDO:

Que, de acordo com o artigo 19 da Lei nº 27.275, a AGÊNCIA DE ACESSO À INFORMAÇÃO PÚBLICA (AAIP), entidade autárquica com autonomia funcional no âmbito do CHEFE DO GABINETE DE MINISTROS, é a Autoridade de Execução da Lei de Proteção de Dados Pessoais nº 25.326, entre outras atribuições.

Que, de acordo com o artigo 29, alínea b), da Lei nº 25.326, a AAIP tem entre suas atribuições para emitir as normas e regulamentos que devem ser observados para o correto tratamento de dados pessoais.

Que o artigo 12 do Anexo I do Decreto nº 1558/01 autoriza a Direção Nacional de Proteção de Dados Pessoais (DNPDP) a avaliar, de ofício ou a pedido de uma parte interessada, o nível de proteção proporcionado pela regulamentação de um Estado ou organização internacional.

Que a mesma regra afirma que

> A adequação do nível de proteção assegurado por um país ou organismo internacional será avaliada em função de todas as circunstâncias de uma transferência ou de uma categoria de transferências de dados; em especial, devem ser tidas em conta a natureza dos dados, a finalidade e a duração do tratamento ou tratamento previsto, o local de destino final, as normas jurídicas gerais ou setoriais em vigor no país em causa, bem como as normas profissionais, os códigos de conduta e as medidas de segurança em vigor nesses locais ou que sejam aplicáveis a organizações internacionais ou supranacionais.

O que, da mesma forma, prevê que

> um Estado ou organização internacional assegura um nível de proteção adequado quando essa proteção deriva diretamente do ordenamento jurídico vigente, ou dos sistemas de autorregulação, ou da proteção estabelecida pelas cláusulas contratuais que preveem a proteção de dados pessoais.

Que, na ausência de uma decisão de adequação, a legislação admite como garantias adequadas para fins de transferência internacional de dados pessoais a existência de autorregulação ou cláusulas contratuais que ofereçam garantias de proteção comparáveis às de nossos regulamentos.

Que por meio do Provimento DNPDP nº 60/2016, alterado pela Resolução AAIP nº 34/2019, foram aprovadas as cláusulas contratuais-tipo de transferência internacional para cessão e prestação de serviços, incorporadas nos Anexos I e II da referida medida, respectivamente, a fim de garantir um nível adequado de proteção de dados pessoais nos termos do artigo 12 da Lei nº 25.326 e do Anexo I do Decreto nº 1558/01 nas transferências de dados destinadas a países sem legislação adequada.

Esse Anexo I da referida Disposição contém o "Modelo de Contrato de Transferência Internacional de Dados Pessoais para Fins de Transferência de Dados Pessoais", enquanto o Anexo II estabelece o "Modelo de Contrato de Transferência Internacional de Dados Pessoais para Fins de Prestação de Serviços".

Que, tendo em conta a emergência de uma nova geração de legislação em matéria de proteção de dados, o crescimento significativo dos fluxos transfronteiriços e o seu impacto na economia mundial, se registaram pro-

gressos a nível regional e internacional na atualização das cláusulas contratuais-modelo para a transferência internacional, com o objetivo de conduzir à convergência dos instrumentos, simplificar os procedimentos e estabelecer pisos de garantia comuns que reforcem a confiança entre os diferentes países.

Que sejam destacadas as cláusulas contratuais modelo para a transferência internacional de dados pessoais da Rede Ibero-Americana de Proteção de Dados, aprovadas por unanimidade em dezembro de 2021; as Cláusulas Contratuais Padrão da Comissão da União Europeia, de junho de 2021; as cláusulas contratuais modelo da ASEAN para fluxos de dados transfronteiriços, janeiro de 2021; o Contrato Padrão para a Exportação de Informações Pessoais da Administração do Ciberespaço da China, promulgado em fevereiro de 2023 e o primeiro módulo das Cláusulas Contratuais Modelo do Conselho da Europa para Fluxos de Dados Transfronteiriços, aprovado em junho de 2023.

Que a AAIP faz parte da Rede Ibero-Americana de Proteção de Dados (RIPD) e é membro de seu comitê executivo.

Em 22 de outubro de 2021, foi realizada a XIX Reunião da RIPD, em cuja declaração final os Estados ibero-americanos, bem como os empresários, foram instados a levar em consideração as Cláusulas Contratuais Modelo desenvolvidas pela Rede sobre transferências internacionais, especialmente para transferências para jurisdições que não possuem legislação adequada.

Que outros países da região – como o Uruguai, por meio da Resolução nº 50/2022, ou o Peru, por meio da Resolução Diretora nº 074-2022-JUS/DGTAIPD – decidiram adotar esses modelos contratuais, o que permite a padronização de instrumentos para transferências seguras de dados e, ao mesmo tempo, facilita a harmonização regulatória entre as diferentes autoridades de aplicação da lei na região.

Que a Resolução AAIP nº 94/2023 aprovou o Plano Estratégico da AAIP 2022-2026, onde o objetivo para o ano corrente era atualizar as cláusulas contratuais modelo para transferências internacionais de dados pessoais.

Que estas cláusulas permitem cumprir os princípios da proteção de dados pessoais, e proporcionam às empresas ou organizações uma alternativa economicamente viável, evitando que tenham de negociar acordos individuais, permitindo-lhes utilizar um conjunto de cláusulas previamente aprovadas pela Autoridade de Execução.

Que as cláusulas-modelo aqui propostas expressam as duas alternativas práticas mais comuns de uma transferência internacional, como as transferências entre controladores e controladores, ou entre controladores e processadores, propondo modelos de cláusulas-padrão diferenciadas para ambos os casos.

Que também sejam compatíveis com as cláusulas contratuais padrão aprovadas pelo Provimento DNPDP nº 60/2016, e tenham o potencial de contribuir para a convergência regulatória para a adequada proteção de dados, seguindo padrões globalmente aceitos.

Que, pelas razões indicadas, é oportuno e conveniente incorporar as cláusulas contratuais modelo para a transferência internacional de dados pessoais da Rede Ibero-Americana de Proteção de Dados no marco regulatório aplicável em nosso país sobre proteção de dados pessoais.

Que, de acordo com o disposto no artigo 7º, alínea d), da Lei nº 19.549, a Direção de Assuntos Jurídicos da AAIP tomou a intervenção de sua competência.

Que esta medida seja emitida em virtude das competências conferidas pelo artigo 29, § 1º, alínea b) da Lei nº 25.326 e 29 do Decreto nº 1558/2001.

Portanto

O DIRETOR DA AGÊNCIA DE ACESSO À INFORMAÇÃO PÚBLICA

RESOLVE:

ARTIGO 1º - Aprovar as cláusulas contratuais modelo para transferências internacionais incluídas no "Guia para a Implementação de Cláusulas Contratuais Modelo para a Transferência Internacional de Dados Pessoais" (TIDP) que, como Anexo I (IF-2023-108581614-APN-DNPDP#AAIP), é parte integrante desta resolução.

ARTIGO 2º - O presente regulamento entra em vigor a partir da sua publicação no DIÁRIO OFICIAL.

ARTIGO 3º - Deve ser comunicada, publicada, entregue à DIREÇÃO NACIONAL DO REGISTRO OFICIAL e, oportunamente, arquivada. Beatriz de Anchorena. Diretor Geral da AAIP.

MINISTÉRIO DA JUSTIÇA E DIREITOS HUMANOS
DIREÇÃO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS

Provisão 60 - E/2016

Cidade de Buenos Aires, 16/11/2016

TENDO VISTO EX-2016-00311578--APN-DNPDP#MJ e as competências conferidas a esta Direção Nacional pela Lei nº 25.326 e seu Decreto Regulamentador nº 1558, de 29 de novembro de 2001, e

CONSIDERANDO:

Que o artigo 12 do Anexo I do Decreto nº 1558/01 autoriza a DIREÇÃO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS a "avaliar, de ofício ou a pedido de uma parte interessada, o nível de proteção proporcionado pela regulamentação de um Estado ou organização internacional".

Que o mesmo regulamento estabelece que "a adequação do nível de proteção oferecido por um país ou organização internacional será avaliada à luz de todas as circunstâncias que ocorram em uma transferência ou em uma categoria de transferências de dados; em especial, devem ser tidas em conta a natureza dos dados, a finalidade e a duração do tratamento ou tratamento previsto, o local de destino final, as normas jurídicas gerais ou setoriais em vigor no país em causa, bem como as normas profissionais, os códigos de conduta e as medidas de segurança em vigor nesses locais ou que sejam aplicáveis a organizações internacionais ou supranacionais".

Também prevê "que um Estado ou organização internacional forneça um nível adequado de proteção quando tal proteção derive diretamente do sistema jurídico em vigor, ou de sistemas de autorregulação, ou da proteção estabelecida pelas cláusulas contratuais que preveem a proteção de dados pessoais".

Que, por estes motivos, a nossa legislação admite como garantias adequadas para efeitos de transferência internacional de dados pessoais a existência de autorregulação ou cláusulas contratuais que prevejam uma proteção semelhante à dos nossos regulamentos.

Que para estes efeitos é pertinente determinar as garantias e requisitos necessários para que as cláusulas contratuais protejam adequadamente os dados pessoais que são transferidos para países sem legislação adequada nos termos do artigo 12º do Anexo I do Decreto nº 1558/01.

Que esta Direção Nacional entenda que os direitos do titular dos dados pessoais serão melhor garantidos através da aprovação de um modelo de contrato de transferência internacional, tanto para os casos de cessão

como para os de prestação de serviços, que deve ser adotado por quem deve realizar transferências internacionais de dados.

Que, da mesma forma, vale a pena considerar os casos em que o controlador de dados decide se afastar do modelo proposto, situação em que se considera adequado exigir a apresentação do contrato de transferência internacional a esta Direção Nacional para aprovação, a fim de proteger adequadamente os direitos dos titulares dos dados a serem transferidos.

Que, para efeitos da elaboração de contratos-tipo, deve ser tida em conta a experiência internacional, em especial as conclusões do documento de trabalho sobre transferências de dados pessoais para países terceiros do GRUPO de TRABALHO sobre o artigo 29.º da Directiva 95/46/CE, de 24 de Julho de 1998, e as cláusulas contratuais-tipo da COMISSÃO DA COMUNIDADE EUROPEIA constantes da Decisão 2001/497/CE, de 15 de Julho de 1998. Junho de 2001 e Decisão 2010/87/UE de 5 de Fevereiro de 2010.

Que é necessário distinguir nas cláusulas-padrão as duas alternativas práticas mais comuns de uma transferência internacional, como a transferência de dados pessoais e a prestação de serviços, propondo modelos de cláusulas-tipo diferenciadas para ambos os casos.

Que para efeitos da aplicação desta medida, é conveniente determinar os países que, na opinião desta DIREÇÃO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS, possuem legislação adequada.

Que no arquivo EXP-S04:0071111/2011, foi analisada a legislação desses países classificada como legislação adequada pela UNIÃO EUROPEIA, concluindo-se no nível equivalente das regulamentações desses países com relação à Lei nº 25.326.

Que é aconselhável informar o público dos países com legislação apropriada através do site da DIREÇÃO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS, especialmente se for levado em conta que a definição da adequação de um país em relação à legislação argentina é uma matéria que pode sofrer variações periódicas.

Que se deve enfatizar que o reconhecimento de certos países como tendo legislação adequada não implicará uma qualificação, em relação a todos os outros países não incluídos nessa lista, como nações que não possuem tal legislação adequada.

Que a DIREÇÃO GERAL DE ASSUNTOS JURÍDICOS deste Ministério tomou a intervenção de sua competência.

Que esta medida seja emitida no uso dos poderes conferidos pelo artigo 29, parágrafo 1º, alínea b) da Lei nº 25.326 e pelo artigo 29, parágrafo 5º, alínea a) e 12 do Anexo I do Decreto nº 1558/01.

Portanto

O DIRETOR NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS

TEM:

ARTIGO 1º - São aprovadas as cláusulas contratuais-tipo de transferência internacional para atribuição e prestação de serviços incorporadas nos Anexos I e II, que fazem parte integrante desta medida, respectivamente, a fim de garantir um nível adequado de proteção de dados pessoais nos termos do artigo 12 da Lei nº 25.326 e do Anexo I do Decreto nº 1558/01 nas transferências de dados para países sem legislação adequada.

ARTIGO 2º - Prevê-se que os controladores de dados que realizarem transferências de dados pessoais para países que não possuam legislação adequada nos termos do artigo 12 da Lei nº 25.326 e seu Decreto Regulamentador nº 1558/01, e utilizarem contratos diferentes dos modelos aprovados no artigo anterior ou que não contenham os princípios, garantias e conteúdos relacionados com a proteção de dados pessoais previstos nos formulários aprovados, devem solicitar a sua aprovação perante esta Direção Nacional, apresentando-os, o mais tardar, no prazo de TRINTA (30) dias corridos após a sua assinatura.

ARTIGO 3º - Para efeitos da aplicação desta disposição, consideram-se titulares de legislação adequada: Estados-Membros da UNIÃO EUROPEIA e membros do Espaço Econômico Europeu (EEE), CONFEDERAÇÃO SUÍÇA, GUERNSEY, JERSEY, ILHA DE MAN, ILHAS FAROÉ, CANADÁ apenas no que diz respeito ao seu setor privado, PRINCIPADO DE ANDORRA, NOVA ZELÂNDIA, REPÚBLICA ORIENTAL DO URUGUAI e ESTADO DE ISRAEL apenas no que diz respeito aos dados que recebem tratamento automatizado. Esta lista será revista periodicamente por esta Direção Nacional, publicando a lista e as suas atualizações no seu site oficial.

ARTIGO 4º - Deve ser comunicada, publicada, entregue à Direcção Nacional do Registo Oficial e arquivada. — EDUARDO BERTONI, Diretor Nacional, Direção Nacional de Proteção de Dados Pessoais, Ministério da Justiça e Direitos Humanos.

AGÊNCIA DE ACESSO À INFORMAÇÃO PÚBLICA

Resolução 34/2019

RESOL-2019-34-APN-AAIP

Cidade de Buenos Aires, 22/02/2019

TENDO EM CONTA O EX-2019-02190972--APN-AAIP e DNPDP Provisão nº DI-2016-60-E-APN-DNPDP#MJ, Lei nº 25.326 sobre Proteção de Dados Pessoais e seu Decreto Regulamentar nº 1558 de 29 de novembro de 2001, Lei nº 27.275 e Decretos nº 206 de 27 de março de 2017, nº 746 de 25 de setembro de 2017 e nº 899 de 3 de novembro de 2017, e

CONSIDERANDO:

Que a Lei nº 25.326 de Proteção de Dados Pessoais tem por objetivo "a proteção integral dos dados pessoais armazenados em arquivos, registros, bancos de dados ou outros meios técnicos de tratamento de dados, públicos ou privados, destinados à prestação de relatórios, a fim de garantir o direito à honra e à privacidade das pessoas, bem como o acesso às informações que nelas estiverem registradas, de acordo com o disposto no artigo 43, parágrafo terceiro da Constituição Nacional" (artigo 1º, Lei nº 25.326).

O Decreto nº 1558, de 29 de novembro de 2001, que regulamenta a Lei nº 25.326, criou a DIREÇÃO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS, vinculada à SECRETARIA DE JUSTIÇA E ASSUNTOS LEGISLATIVOS do MINISTÉRIO DA JUSTIÇA E DOS DIREITOS HUMANOS, como órgão fiscalizador da referida Lei (Anexo I, artigo 29º do Decreto nº 1558/2001).

Que, por outro lado, a Lei nº 27.275 sobre o Direito de Acesso à Informação Pública criou a AGÊNCIA DE ACESSO À INFORMAÇÃO PÚBLICA ("AAIP") como entidade autárquica com autonomia funcional no âmbito do CHEFE DO GABINETE DE MINISTROS, a fim de "zelar pelo cumprimento dos princípios e procedimentos estabelecidos na Lei [nº 27.275], garantir o exercício efetivo do direito de acesso à informação pública e promover medidas ativas de transparência" (artigo 19, Lei nº 27.275).

Que o Decreto nº 746, de 25 de setembro de 2017, substituiu o artigo 19 da Lei nº 27.275, atribuindo à AGÊNCIA DE ACESSO À INFORMAÇÃO PÚBLICA o poder de atuar como Autoridade de Execução da Lei nº 25.326, e foi incorporado como inciso t) ao artigo 24 da Lei nº 27.275, a

competência da AAIP para "[f]iscalizar a proteção integral dos dados pessoais registrados em arquivos, registros, bancos de dados ou outros meios técnicos de tratamento de dados, públicos ou privados, destinados a fornecer relatórios, para garantir o direito à honra e à privacidade dos indivíduos, bem como o acesso às informações registradas sobre eles".

Que, da mesma forma, o Decreto nº 899, de 3 de novembro de 2017, substituiu o artigo 29 do Anexo I do Decreto nº 1558/01, estabelecendo que "a AGÊNCIA DE ACESSO À INFORMAÇÃO PÚBLICA, nos termos do artigo 19 da Lei nº 27.275, substituído pelo artigo 11 do Decreto nº 746/17, é o órgão de controle da Lei nº 25.326" (artigo 1º, Decreto nº 899/2017).

Que, entre as atribuições atribuídas à AGÊNCIA DE ACESSO À INFORMAÇÃO PÚBLICA está a de emitir as normas e regulamentos que devem ser observados no desenvolvimento das atividades incluídas na Lei 25.326 (artigo 29, parágrafo 1.b) da Lei nº 25.326).

Que a então DIREÇÃO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS, subordinada ao Ministério da Justiça e dos Direitos Humanos, emitiu o Provimento 60 – E/2016 pelo qual foi aprovado um modelo de contrato de transferência internacional, tanto para os casos de transferência de dados pessoais como para os casos de prestação de serviços, de forma a garantir um nível adequado de proteção dos dados pessoais nos termos do artigo 12º da Lei Nº 25.326 nessas transferências de dados para países sem legislação adequada.

Que, da mesma forma, a Provisão 60 - E/2016 determinou os países que possuem legislação adequada, e acrescentou a possibilidade de que a lista seja revisada periodicamente pela então DIREÇÃO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS, publicando a lista e suas atualizações em seu site oficial.

Que, em particular, o artigo 3º da Provisão 60 – E/2016 estabelece que "[n]o que respeita aos fins de aplicação desta disposição, consideram-se países com legislação adequada os seguintes países: Estados-Membros da UNIÃO EUROPEIA e membros do Espaço Econômico Europeu (EEE), CONFEDERAÇÃO SUÍÇA, GUERNSEY, JERSEY, ILHA DE MAN, ILHAS FAROÉ, CANADÁ apenas no que diz respeito ao seu setor privado, PRINCIPADO DE ANDORRA, NOVA ZELÂNDIA, REPÚBLICA ORIENTAL DO URUGUAI e ESTADO DE ISRAEL apenas no que diz respeito aos dados que recebem tratamento automatizado."

Que foi recebida uma solicitação do DEPARTAMENTO DE SERVIÇOS DIGITAIS, CULTURA, MÍDIA E ESPORTE DO REINO UNIDO DA GRÃ-BRETANHA E IRLANDA DO NORTE, solicitando à AGÊNCIA DE ACESSO À INFORMAÇÃO PÚBLICA que adote as medidas necessárias para garantir que o fluxo internacional de dados pessoais da REPÚBLICA ARGENTINA para o REINO UNIDO DA GRÃ-BRETANHA E IRLANDA DO NORTE seja mantido ininterrupto após a partida do REINO UNIDO DA GRÃ-BRETANHA E DA IRLANDA DO NORTE da UNIÃO EUROPEIA.

Que, de acordo com o que foi relatado na respectiva solicitação e de acordo com a revisão de antecedentes da AGÊNCIA DE ACESSO À INFORMAÇÃO PÚBLICA, os padrões de proteção de dados pessoais fornecidos pelo REINO UNIDO DA GRÃ-BRETANHA E IRLANDA DO NORTE foram mantidos e até reforçados com relação à situação regulatória do Estado requerente no momento em que a então DIREÇÃO NACIONAL DE A PROTEÇÃO DE DADOS PESSOAIS teria decidido incluir os Estados-Membros da UNIÃO EUROPEIA - incluindo o REINO UNIDO DA GRÃ-BRETANHA E IRLANDA DO NORTE - na lista de países com legislação apropriada (Artigo 3 da Disposição 60 - E/2016).

Que, pelas razões expostas acima, a AGÊNCIA DE ACESSO À INFORMAÇÃO PÚBLICA considera que o REINO UNIDO DA GRÃ-BRETANHA E IRLANDA DO NORTE continua a oferecer um nível adequado de proteção nos termos da Lei nº 25.326.

Que, consequentemente, a AGÊNCIA DE ACESSO À INFORMAÇÃO PÚBLICA considera apropriado revisar a lista de países com legislação adequada contemplada no Artigo 3 da Disposição 60 - E/2016 e incluir o REINO UNIDO DA GRÃ-BRETANHA E IRLANDA DO NORTE nessa lista.

Que a DIREÇÃO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS e a COORDENAÇÃO DE ASSUNTOS JURÍDICOS da AGÊNCIA DE ACESSO À INFORMAÇÃO PÚBLICA tomaram a intervenção de sua competência.

Que este seja emitido no uso dos poderes conferidos pelo artigo 29, parágrafo 1.b) da Lei nº 25.326.

Por esse motivo, o

DIRETOR DA AGÊNCIA DE ACESSO À INFORMAÇÃO PÚBLICA

RESOLVE:

ARTIGO 1º: O artigo 3º da Provisão 60 - E/2016 passa a ter a seguinte redação: "Para efeitos da aplicação da presente disposição, consideram-se países com legislação adequada os seguintes países: Estados-Membros da UNIÃO EUROPEIA e membros do Espaço Econômico Europeu (EEE), REINO UNIDO DA GRÃ-BRETANHA E IRLANDA DO NORTE, CONFEDERAÇÃO SUÍÇA, GUERNSEY, JERSEY, ILHA DE MAN, ILHAS FAROE, CANADÁ apenas no que diz respeito ao seu setor privado, PRINCIPADO DE ANDORRA, NOVA ZELÂNDIA, REPÚBLICA ORIENTAL DO URUGUAI e ESTADO DE ISRAEL apenas no que diz respeito aos dados que recebem tratamento automatizado.

ARTIGO 2º- Deve ser comunicado, publicado, entregue à DIREÇÃO NACIONAL DO REGISTRO OFICIAL e arquivado. Eduardo Andrés Bertoni

Capítulo 3
Por que e como Construir uma Convenção Interamericana sobre Autodeterminação Informativa, Tratamento e Circulação de Dados Pessoais

Introdução

Como explicamos no capítulo 1 desta obra, a necessidade de regular adequadamente o fluxo livre de dados pessoais, permitindo-o, mas ao mesmo tempo garantindo a proteção desses dados, exige normas harmonizadas na região.

Isso leva à proposta de normas unificadas em nível regional, aproveitando os marcos regionais existentes e considerando se é necessário usar o sistema de tratados internacionais vigentes (*hard law*) ou um marco mais flexível, fácil e rápido de implementar, como um acordo realizado por meio de agências de dados pessoais (*soft law*). Cada opção tem suas vantagens e desvantagens.

Em relação a isso, a RIPD elaborou os Padrões em 2017, mas estes não serviram como guia para forçar os países da região a aprovar marcos legais. De fato, o padrão mais influente continua sendo o RGPD europeu.

Por outro lado, a RIPD elaborou as cláusulas-padrão contratuais (SCC) como uma forma de harmonizar o uso da ferramenta contratual nas TIDP. No entanto, ainda falta um desenvolvimento mais detalhado que inclua outras ferramentas, como as normas corporativas vinculantes, códigos de certificação ou normas regionais subscritas por todos os países da região. Isso pode ser alcançado se todos os países da região concordarem com um marco comum para a proteção de dados e a transferência intrarregional desses dados. Esse objetivo poderia ser alcançado por meio do sistema interamericano de Direitos Humanos.

1 Sistema interamericano de direitos humanos

1.1 Introdução

No que diz respeito aos acordos dentro dos marcos regionais, encontramos várias estruturas legais existentes que poderiam acomodar esse arranjo, como é o caso da OEA, do Pacto Andino ou do Mercosul.

Ao contrário dos dois últimos, o primeiro tem uma cobertura muito maior, abrangendo um total de 34 países. Além disso, a OEA já tem precedentes tanto em termos de princípios de proteção de dados pessoais quanto de acesso à informação pública e desempenhou um papel em numerosos tratados e acordos regionais de direitos humanos, como a Convenção Americana sobre Direitos Humanos[121] (Pacto de San José da Costa Rica), a Convenção Interamericana para Prevenir e Punir a Tortura, a "Convenção de Belém do Pará" ou Convenção Interamericana para Prevenir, Punir e Erradicar a Violência Contra a Mulher, e a Convenção Interamericana sobre o Desaparecimento Forçado de Pessoas.

No entanto, também é possível argumentar que o esforço para desenvolver um marco regional pode começar em nível plurilateral, por um grupo específico de países com interesses afins, sem depender da estrutura de uma organização intergovernamental pré-existente. De fato, tanto a base normativa quanto as autoridades competentes para a implementação de normas relacionadas à proteção de dados já existem na maioria dos países latino-americanos. Portanto, podemos argumentar que um esforço multilateral pode ser potencialmente bem-sucedido.

1.2 Vantagens de um tratado internacional na região

A possibilidade de que a América Latina tenha um tratado internacional sobre proteção de dados pessoais e privacidade é muito importante e vantajosa pelas seguintes razões.

121 **A Convenção Americana sobre Direitos Humanos** é um tratado internacional adotado pela Organização dos Estados Americanos (OEA) em 1969 e entrou em vigor em 1978. Seu principal objetivo é estabelecer os direitos e liberdades fundamentais que devem ser respeitados e protegidos pelos Estados partes.

Em primeiro lugar, unifica as regras em nível regional, permitindo que sejam sancionadas por países que ainda não as têm. Um tratado regional ajudará no crescimento do direito à proteção de dados na região, regulamentando questões internacionais, como transferências internacionais de dados, facilitando o livre fluxo de dados (tema central para o comércio internacional) e a colaboração direta entre autoridades de proteção de dados dentro de um marco regulamentado (algo que já ocorre de fato na região, como evidenciam os casos da *OpenAI*).

Além disso, facilita o desenvolvimento da proteção de dados como um direito fundamental, já que o tratado poderia encarregar a Corte Interamericana de atuar como órgão transnacional interpretativo dos direitos contidos no acordo, com efeito vinculante. Isso forçaria os Estados-membros a realizar um controle de convencionalidade de suas respectivas leis em relação ao tratado, resultando em maior harmonização na América Latina.

O tratado poderia prever a criação de um organismo consultivo e emissor de *soft law*, similar ao "Data Protection Committee" da Convenção 108 ou à Comissão Interamericana de Mulheres, com a obrigação de incluir medidas positivas, como propõe a Convenção de Belém do Pará.

O projeto de tratado propõe, então, a criação de uma Comissão Interamericana de Proteção de Dados Pessoais (CIPDP) como órgão intergovernamental criado dentro da OEA para garantir o reconhecimento dos direitos humanos dos titulares de dados pessoais e como um fórum político hemisférico para os direitos dos titulares de dados, com a participação das autoridades nacionais de dados pessoais de cada país membro. A CIPDP poderia ser um organismo emissor de *soft law*, algo muito importante devido à complexidade e às mudanças constantes nessa área.

Finalmente, a existência do tratado, uma vez aprovado e em vigor, permitirá a criação de um bloco regional de 34 países latino-americanos com um sistema de proteção de dados homogêneo, que protegerá os habitantes da região (um total de 660 milhões de pessoas) e permitirá que a região se posicione frente a outros blocos regionais de maneira diferente da posição individual existente atualmente. Tudo isso com o objetivo de negociar reconhecimentos de adequação em nível regional.

2 Proposta de uma convenção interamericana sobre autodeterminação informativa, tratamento e circulação de dados pessoais

2.1 Fontes

O texto do projeto se baseia nos Princípios da OEA de 2021. Em 2021, a Assembleia Geral da Organização dos Estados Americanos (OEA) aprovou os Princípios Atualizados sobre Privacidade e Proteção de Dados Pessoais. Esses princípios visam identificar os elementos básicos de uma proteção eficaz.

Assim, a OEA, ao apresentar os princípios, afirma:

> os Princípios Atualizados sobre Privacidade e Proteção de Dados Pessoais, como instrumento de soft law interamericano, têm como objetivo servir como referência para os Estados-membros fortalecerem seus respectivos marcos jurídicos na matéria, além de orientar o desenvolvimento coletivo da região em direção a uma proteção harmônica e eficaz dos dados pessoais.

Também são considerados os Padrões Ibero-americanos de proteção de dados, elaborados pela RIPD em 2017, bem como a Convenção 108 modernizada e o RGPD europeu.

Todos esses documentos contêm uma série de princípios muito semelhantes, apesar de suas diferentes redações e contextos. O espírito desses documentos é o mesmo: proteger os dados das pessoas por meio dos mecanismos usuais encontrados nesse ramo do Direito.

O projeto de tratado tem como base a Convenção 108 modernizada, mas também a CADH e os mecanismos de direito internacional reconhecidos na Convenção de Belém do Pará. Incluem-se, por fim, na parte geral, as cláusulas usuais para esse tipo de tratado interamericano, como aquelas relacionadas à entrada em vigor, denúncia etc.

2.2 Conteúdo

Nossa proposta de Convenção Interamericana sobre Proteção de Dados parte da premissa de que todo tratado internacional sobre proteção de dados pessoais deve conter pelo menos as seguintes seções fundamentais:

- Uma parte geral, com definições e princípios, onde estabelece os objetivos e princípios gerais do tratado, como a proteção da privacidade e de outros direitos fundamentais, a transparência e a segurança no tratamento de dados, e a integridade dos dados pessoais. Também define conceitos-chave, como "dados pessoais", "tratamento de dados", "controlador dos dados" e "titular dos dados".
- A definição do âmbito de aplicação, incluindo segurança nacional, especificando quem está sujeito às disposições e quais tipos de dados pessoais estão protegidos. Também aborda a segurança nacional, estabelecendo limites e condições para a coleta e tratamento de dados pessoais relacionados à segurança do Estado.
- A definição de direitos dos titulares de dados, pela qual se estabelece os direitos fundamentais das pessoas cujos dados pessoais estão sendo tratados, como o direito de acesso, retificação, cancelamento e oposição, bem como o direito à portabilidade de dados e a não ser objeto de decisões automatizadas.
- A previsão de obrigações para o setor público e privado, visando garantir a proteção dos dados pessoais. Isso inclui a implementação de medidas de segurança, transparência e responsabilidade adequadas, a designação de um encarregado pela proteção de dados e a realização de relatórios de impacto na proteção de dados.
- A regulação explícita da transferência internacional de dados, estabelecendo as condições e procedimentos para a transferência de dados pessoais entre países, garantindo o respeito às normas de proteção de dados pessoais previstas no tratado.
- A previsão de mecanismos de *enforcement* dos direitos reconhecidos, assegurando o cumprimento das disposições do tratado, incluindo a criação de autoridades de supervisão e controle, a imposição de sanções e a resolução de controvérsias.
- A criação de agências independentes de proteção de dados pessoais, responsáveis pela supervisão e controle da aplica-

ção do tratado, bem como pelo recebimento e investigação de queixas dos titulares de dados.

- A coordenação entre agências de proteção de dados pessoais, com a implementação de mecanismos de cooperação para garantir a aplicação efetiva e uniforme do tratado.
- O esclarecimento de questões gerais de todos os tratados, como sua entrada em vigor, denúncia, resolução de controvérsias e outras disposições finais.

2.3 Direitos substantivos

Uma Convenção regional deve assegurar, no mínimo, os direitos definidos como "ARCO" nas legislações latino-americanas, bem como os novos direitos previstos nas normas de segunda geração, definidos como "POL".

Os direitos ARCO são um conjunto de garantias que se referem a:

- Acesso (A): Direito de acessar os dados pessoais em posse de terceiros e obter informações sobre sua origem e destino.
- Retificação (R): Direito de corrigir ou retificar dados pessoais imprecisos ou incompletos.
- Cancelamento (C): Direito de cancelar ou excluir dados pessoais que não sejam mais necessários ou não estejam sendo usados de acordo com a finalidade original.
- Oposição (O): Direito de se opor ao tratamento de dados pessoais quando as normas de proteção de dados não estejam sendo respeitadas.

Os direitos POL são garantias adicionais, de última geração, que incluem:

- Portabilidade (P): Direito de receber dados pessoais em formato estruturado e comumente utilizado, e de transmiti-los a outro controlador.
- Esquecimento (O): Direito de solicitar a exclusão ou supressão de dados pessoais do titular que não sejam mais relevantes, atuais ou pertinentes.

- Limitação (L): Direito de limitar o tratamento de dados pessoais quando as normas de proteção de dados não estejam sendo respeitadas.

Além disso, o direito à revisão de decisões baseadas em tratamento automatizado de dados pessoais é um direito fundamental que protege os indivíduos contra os efeitos adversos de decisões tomadas exclusivamente com base em tratamento automatizado de dados pessoais, sem intervenção humana. Esse direito garante que os indivíduos possam solicitar a revisão de decisões que os afetem de maneira adversa, como a negação de crédito ou de um pedido de emprego baseado em análise automatizada de dados pessoais, a inclusão em uma lista de pessoas consideradas de "alto risco" com base em um algoritmo que utiliza dados pessoais, ou a tomada de decisões automatizadas que afetam a vida pessoal ou profissional de um indivíduo, como o cancelamento de uma conta ou a revogação de uma autorização.

O direito à revisão de decisões baseadas em tratamento automatizado de dados pessoais busca garantir que as decisões sejam tomadas de maneira justa e transparente, e que os indivíduos possam compreender as razões por trás de uma decisão automatizada que os afeta. Com o exercício desse direito, os indivíduos têm o direito de solicitar a revisão da decisão automatizada, obter informações claras e inteligíveis sobre a lógica usada no tratamento automatizado e obter uma resposta fundamentada sobre a decisão tomada.

2.4 Princípios e obrigações na matéria

Os princípios de proteção de dados são de extrema importância para regulamentar o manejo de informações pessoais, garantindo o respeito à privacidade individual e salvaguardando direitos fundamentais. Esses princípios estabelecem uma base uniforme para regulamentar o tratamento de dados pessoais, impondo obrigações homogêneas independentemente das fronteiras internacionais.

Alguns desses princípios fundamentais, reconhecidos em instrumentos de direito internacional existentes, como a Convenção 108 e a Convenção de Malabo, incluem:

- Tratamento legal e equitativo, segundo o qual os dados pessoais devem ser tratados de acordo com a lei e de forma justa;
- Necessidade de consentimento informado ou outra base legal para o tratamento, devendo o consentimento ser obtido de maneira livre, específica e consciente;
- Finalidade definida, segundo o qual os dados devem ser coletados apenas para fins específicos e legítimos, e qualquer tratamento posterior deve estar alinhado com essas finalidades declaradas;
- Minimização de dados, segundo o qual apenas os dados pessoais relevantes e necessários devem ser tratados;
- A qualidade dos dados, de forma que os dados pessoais devem ser precisos e, se necessário, atualizados para garantir sua confiabilidade;
- Restrição de armazenamento, segundo o qual os dados pessoais não devem ser armazenados por períodos mais longos do que o necessário, estabelecendo um limite de retenção;
- A necessidade de implementação de medidas de segurança robustas: para proteger os dados pessoais contra acesso ou modificação não autorizados.

Além desses princípios, há obrigações cruciais que acompanham o tratamento de dados pessoais, operacionalizando os princípios mencionados acima. Tais obrigações incluem garantir aos titulares de dados:

- Os direitos de acesso, retificação, cancelamento e oposição (ARCO), bem como a portabilidade, o esquecimento e a limitação (POL) do tratamento de seus dados pessoais. A violação desses direitos também obriga a compensar qualquer dano resultante de uma violação de dados.
- A exigência de consentimento, especialmente considerando a necessidade de consentimento explícito em casos de tratamento de dados pessoais sensíveis.
- A transparência, proporcionando informações claras e acessíveis sobre o tratamento de seus dados pessoais.

- A segurança, aplicando salvaguardas técnicas e organizacionais apropriadas para proteger os dados pessoais contra possíveis ameaças.

Essas obrigações também incluem a garantia da segurança transfronteiriça das transferências de dados pessoais. Esses princípios e obrigações são a base para construir uma abordagem responsável ao tratamento de dados pessoais, promovendo o fluxo livre de dados com confiança. Eles buscam proteger os direitos dos titulares de dados e proporcionar segurança jurídica às pessoas, ao mesmo tempo em que fomentam um ambiente digital seguro para o intercâmbio internacional de dados. Portanto, atuam como uma pedra angular para que os países estabeleçam marcos sólidos de proteção de dados.

Finalmente, consideramos relevante incluir o princípio da precaução. Este princípio é relevante quando há falta de certeza sobre os potenciais danos do tratamento de dados pessoais que possam causar um dano grave e irreversível, de modo que os Controladores dos Dados devem abster-se de realizar tal tratamento ou adotar medidas preventivas para proteger os direitos do titular dos dados, sua dignidade humana e outros direitos humanos. O princípio da precaução também se aplicaria quando o risco ou a magnitude do dano produzido ou que pode ocorrer não são conhecidos com antecedência, porque não há maneira de estabelecer, a médio ou longo prazo, os efeitos de um tratamento de dados.

2.5 Transferência internacional, cumprimento e colaboração

O projeto de tratado visa não apenas proteger os dados pessoais, mas também permitir o livre fluxo desses dados dentro da região. Para isso, estabelece-se a regra de proibir transferências para países que não tenham proteção adequada, permitindo, entretanto, a livre circulação de dados entre os países-membros, partindo do princípio de que a assinatura do tratado introduz no país uma norma protetora que o torna adequado.

O reconhecimento de direitos fundamentais sem um meio adequado de efetivá-los deixaria tais direitos sem valor prático. Por isso, propõem-se tanto ações de cumprimento dos direitos reconhecidos, como o habeas

data, quanto a obrigação de prevenir a continuação do dano e de indenizar o titular dos dados pessoais pelo tratamento inadequado dos mesmos. Além disso, é crucial que a Convenção regional articule as relações entre as agências, visando melhorar a cooperação internacional na investigação de infrações, assegurando o respeito aos direitos em nível regional.

Nesse contexto, acreditamos que a aprovação de um tratado internacional sobre o tema certamente incentivará os países que ainda não possuem normas a adotá-las. Por outro lado, terá um efeito unificador nos critérios interpretativos se conseguirmos criar organismos internos de interpretação e de elaboração de *soft law*, similar ao EDPB.

3 Conclusões

Existem diversos elementos normativos e institucionais que os países latino-americanos precisam enfrentar para realizar transferências internacionais de dados pessoais. Os casos de Argentina, Brasil, Colômbia, México e Uruguai, explorados no primeiro capítulo, são particularmente interessantes para entender a complexidade dos regimes de transferência de dados na região. Seus marcos nacionais mostram como diferenças relativamente pequenas podem criar obstáculos consideráveis para o livre fluxo de dados, sem necessariamente torná-lo mais seguro ou melhorar a segurança jurídica, nem aumentar a autodeterminação informativa dos titulares.

Nossa análise das regulamentações de transferência de dados nesses países permitiu compreender a evolução da proteção de dados na região, destacando a forte influência do modelo europeu, ressaltando os avanços alcançados na proteção dos direitos de privacidade dos dados pessoais dos titulares e, ao mesmo tempo, os inúmeros desafios que ainda persistem.

Nesse contexto, como apontamos desde a introdução, há um número limitado de opções disponíveis para promover fluxos de dados seguros e confiáveis, ao mesmo tempo em que se aumenta a interoperabilidade jurídica dos marcos de proteção de dados na América Latina. É importante destacar que enfatizamos o desenvolvimento de opções sólidas para facilitar fluxos de dados seguros e confiáveis e, ao mesmo tempo, fomentar a interoperabilidade jurídica, o que depende de se acordar princípios compartilhados que, no caso dos países latino-americanos, já sustentam os

marcos nacionais, e, posteriormente, definir as regras apropriadas (e idealmente) compartilhadas: regras que determinam como os controladores e operadores de dados podem tratar dados pessoais.

Claro, esses elementos-chave devem ser complementados por mecanismos adequados que garantam o cumprimento dos princípios e normas. Embora a opção mais tradicional se baseie na adoção de decisões de adequação pelos reguladores nacionais, essa não é necessariamente a opção mais ágil. Essas certificações formais tampouco garantem que os dados pessoais serão tratados adequadamente quando exportados para outros países. A adoção de cláusulas-padrão contratuais, que exploramos no segundo capítulo deste volume, é uma alternativa mais ágil que parece contar cada vez mais com o apoio das autoridades de proteção de dados em todo o mundo.

De fato, essa estratégia surge como uma tática promissora para facilitar os fluxos seguros de dados pessoais na região, criando uma opção aceitável para os reguladores, que podem evitar a necessidade de múltiplas decisões de adequação, que podem ser muito onerosas e não necessariamente coerentes. Essas cláusulas, adotadas pela Rede Ibero-Americana de Proteção de Dados, oferecem mecanismos contratuais padronizados para a transferência de dados pessoais dentro da América Latina ou fora da região, desde que as cláusulas contratuais sejam adotadas, vinculando assim as partes contratuais.

Como enfatizamos, ao adotar cláusulas-padrão contratuais, as empresas e organizações podem navegar pelas complexidades das transferências internacionais de dados de maneira mais eficaz, mitigando os riscos legais, protegendo os direitos das pessoas e promovendo a interoperabilidade jurídica por meio de uma abordagem descentralizada.

No entanto, as decisões de adequação adotadas pelos reguladores nacionais e as disposições contratuais padrão não são as únicas estratégias que a América Latina pode adotar para regular os fluxos de dados de maneira coerente e segura. Sob essa perspectiva, acreditamos que chegou o momento de criar uma "Convenção Interamericana sobre Autodeterminação Informativa, Tratamento e Circulação de Dados Pessoais", como um passo proativo para melhorar e harmonizar os padrões de proteção de dados e promover a cooperação transfronteiriça na região. Consideramos que, entre outros, os Padrões de proteção de dados da RIPD (tanto sua versão atual quanto a atualizada, prevista para 2024) podem ser pontos de partida para a redação da Convenção Interamericana que se propõe.

Propõe-se um modelo dessa Convenção, levando em consideração as melhores práticas estabelecidas pelos instrumentos internacionais existentes, como a Convenção do Conselho da Europa para a proteção das pessoas com relação ao tratamento automatizado de dados pessoais, mais conhecida como Convenção 108, e os Padrões de proteção de dados da RIPD.

Esperamos que a América Latina possa ser reconhecida como líder em proteção de dados e que seu marco regional se torne um "selo de qualidade", como aconteceu com a Europa. De fato, os dois marcos, juntamente com a Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais, mais conhecida como Convenção de Malabo, podem ser vistos como instrumentos que se reforçam mutuamente e aumentam a tendência global em direção a uma governança sólida de dados, com os direitos humanos no centro.

Ao fornecer um marco unificado para harmonizar as regulamentações de proteção de dados nos países latino-americanos, essa convenção estabeleceria princípios, padrões e mecanismos comuns para regular as transferências transfronteiriças de dados. Esse marco importante pode fomentar a confiança, estabelecer um mecanismo significativo de cooperação regional, harmonizar e empoderar indivíduos e empresários, ao mesmo tempo em que aumenta a segurança jurídica e promove a interoperabilidade jurídica por meio de uma abordagem convergente. Além disso, teria a possibilidade de estabelecer um canal oficial de comunicação e cooperação entre as autoridades latino-americanas de proteção de dados, aumentando significativamente a coordenação e a governança regional.

A criação de uma Convenção Interamericana sobre Autodeterminação Informativa, Tratamento e Circulação de Dados Pessoais pode trazer importantes benefícios para a região, mas estamos plenamente cientes da complexidade envolvida na aprovação e implementação de um projeto tão ambicioso. Ao harmonizar as regulamentações de proteção de dados e promover a cooperação transfronteiriça, a convenção facilita transferências de dados ciberseguras e resilientes, melhorando a cooperação em pesquisa e inovação e, consequentemente, estimulando o crescimento econômico.

Além disso, uma Convenção Interamericana fortaleceria a posição da região na economia global de dados, posicionando a América Latina como líder em governança responsável de dados e cooperação digital. Embora reconheçamos que o caminho para o projeto e, em particular, para a assi-

natura e ratificação de um tratado internacional, não seja nada fácil, acreditamos que os benefícios superam amplamente os custos desse esforço.

Sem deixar de ser otimistas, é importante manter uma certa dose de pragmatismo e reconhecer que as convenções regionais, especialmente aquelas que se concentram em um tema tão delicado quanto a proteção de dados, envolvem várias complexidades. A mais óbvia é o considerável esforço diplomático necessário para negociar uma convenção regional, que pode consumir muito tempo e recursos. No entanto, como destacamos nas primeiras páginas deste texto, as partes interessadas latino-americanas, desde governos até empresas, pesquisadores e ativistas, estão muito conscientes dos benefícios que um marco compartilhado de proteção de dados representará.

3.1 Transferências de dados com confiança

Como destacado na introdução deste trabalho, desde a Cúpula do G20 de 2019, em Osaka, os chefes de governo concordaram em trabalhar na visão de fluxo livre de dados com confiança ("*Data Free Flow with Trust*" ou "DFFT").[122] A Declaração dos Líderes de Osaka estabelece que os marcos legais, tanto nacionais quanto internacionais, devem ser respeitados. A necessidade de melhorar a interoperabilidade legislativa entre sistemas legislativos nacionais, para permitir que os dados fluam de forma mais livre e segura, é uma prioridade destacada por um número crescente de estados, tanto a nível latino-americano quanto global.

Em 2021, o Grupo dos 7 (G7) começou a traduzir a importância das transferências transfronteiriças com confiança no Roteiro dos Ministros Digitais e de Tecnologia do G7, que reconhece que a "capacidade de mover e proteger dados através das fronteiras é essencial para o crescimento econômico e a inovação".[123] Conforme destacado, as transferências de dados têm adquirido um papel cada vez mais vital para a economia e a cooperação global. A Câmara de Comércio Internacional estima que a contribuição das

122 G20. **G20 Osaka Leaders' Declaration.** Osaka. 29 de junho de 2019. Disponível em: https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html.

123 G7 DIGITAL AND TECHNOLOGY MINISTERS. **G7 Digital and Technology Track – Annex 2: G7 Roadmap for Cooperation on Data Free Flow with Trus**t. Cornwall. 28 de abril de 2021. Disponível em: http://www.g8.utoronto.ca/ict/2021-annex_2-roadmap.html.

transferências de dados ao PIB mundial seja de cerca de 2,8 trilhões de dólares, com previsão de aumento para 11 trilhões de dólares em 2025.[124] O setor privado e as áreas de pesquisa e desenvolvimento são beneficiários essenciais de mecanismos que permitam uma transferência confiável e segura.

Nesse contexto, a definição de estratégias eficazes e eficientes para permitir fluxos de dados livres e seguros deve ser considerada um objetivo prioritário de políticas públicas, além de ser um tema crucial para a proteção de dados. No entanto, desde as revelações do ex-contratado da Agência de Segurança Nacional, Edward Snowden[125], a confiança nos fluxos internacionais de dados foi cada vez mais corroída pelas preocupações sobre o acesso governamental não regulamentado aos dados pessoais. Em particular, a possibilidade de demandas governamentais de acesso a dados para fins penais e de segurança nacional pode entrar em conflito com os direitos de proteção de dados e comprometer a eficácia dos mecanismos existentes.

Nessa perspectiva, é importante notar que os países latino-americanos participaram de uma forma peculiar do "efeito Bruxelas" seletivo. De fato, o marco da União Europeia para a proteção de dados pessoais é composto por duas leis irmãs: o notório RGPD, o regulamento 2016/679, e a chamada Diretiva Law Enforcement 2016/680, que visa regular como os dados pessoais processados no contexto da segurança nacional e das investigações criminais podem ser armazenados. Curiosamente, todos os países latino-americanos que atualmente possuem marcos de proteção de dados parecem ter esquecido deste último.[126]

Nesse contexto, acreditamos que um elemento essencial a ser considerado para estabelecer transferências de dados verdadeiramente confiáveis é estender a proteção dos dados pessoais à segurança nacional e às investigações criminais. Embora reconheçamos que essas últimas atividades apresen-

124 International Chamber of Commerce. White Paper on Trusted Government Access to Personal Data Held by the Private Sector. **International Chamber of Commerce**. 22 de agosto de 2022. Disponível em: https://iccwbo.org/news-publications/policies-reports/icc-white-paper-on-trusted-government-access-to-personal-data-held-by-the-private-sector/.

125 The Guardian. The NSA Files. Disponível em: https://www.theguardian.com/us-news/the-nsa-files.

126 ABBAS DA SILVA, Lorena, FRANQUEIRA, Bruna Diniz, HARTMANN, Ivar A. O que os olhos não veem, as câmeras monitoram: reconhecimento facial para segurança pública e regulação na América Latina. *Revista Digital De Direito Administrativo*, v. 8, n. 1, p. 171-204, 2021. Disponível em: https://doi.org/10.11606/issn.2319-0558.v8i1p171-204.

tam um caráter especial e precisam ser regulamentadas com uma legislação específica, tal regulamentação deve existir para que se possa afirmar que as transferências de dados podem ser concretamente seguras e confiáveis. Nessa perspectiva, sugerimos que a convenção proposta seja aplicável horizontalmente, tanto a atores públicos quanto privados, e reconheça explicitamente sua aplicabilidade à segurança nacional e às investigações criminais.

3.2 Rumo a uma convenção interamericana sobre autodeterminação informativa, tratamento e circulação de dados pessoais

Uma convenção regional de proteção de dados pode facilitar e, idealmente, aumentar os padrões de proteção de dados nos países participantes, promovendo a tão necessária consistência e coerência nos marcos regulatórios, reduzindo enormemente a insegurança jurídica e os custos de conformidade para as empresas que operam além das fronteiras, facilitando as transferências transfronteiriças de dados e promovendo a integração política regional e o crescimento econômico.

Ao estabelecer princípios, mecanismos e procedimentos compartilhados na América Latina para regular as transferências transfronteiriças de dados, é provável que um marco regional melhore a cooperação em uma variedade de temas, que vão desde a pesquisa até o comércio eletrônico, a cibersegurança e a aplicação da lei, fortalecendo assim a integração econômica e social da região, ao mesmo tempo que aumenta a resiliência contra as ameaças transnacionais e o cibercrime.

Além disso, um marco regional de proteção de dados baseado nos direitos humanos reafirmará, sem dúvida, o compromisso da América Latina de considerar a proteção de dados pessoais como um direito fundamental. Isso aumentaria consideravelmente a credibilidade e a influência de toda a região nos fóruns internacionais, permitindo que os países participantes moldassem debates e padrões globais sobre questões de proteção de dados.

Vale a pena que a América Latina dê esse passo importante. O esforço não será fácil, mas é hora de ser ousados e ambiciosos para criar um instrumento verdadeiramente latino-americano para a governança de dados, com vistas a garantir o devido tratamento dos dados das pessoas na América Latina.

Anexo A – Projeto de Convenção Interamericana sobre Autodeterminação Informativa, Tratamento e Circulação de Dados Pessoais

OS ESTADOS PARTES DA PRESENTE CONVENÇÃO,

RECONHECENDO que o respeito irrestrito aos direitos humanos e à privacidade foi consagrado pela Declaração Americana dos Direitos e Deveres do Homem e pela Declaração Universal de Direitos Humanos e reafirmados em outros instrumentos internacionais e regionais;

RECORDANDO os Princípios Atualizados sobre Privacidade e Proteção de Dados Pessoais elaborado pelo Comitê Jurídico da OEA em 2021 e afirmando que a proteção de dados pessoais transcende todos os setores da sociedade independentemente de sua nacionalidade, residência, classe, raça ou etnia, nível de renda, cultura, escolaridade, idade ou religião;

RECORDANDO que a Corte Interamericana de Direitos Humanos reconheceu o direito à autodeterminação informativa como direito autônomo na decisão Série C nº 506, de 18 de outubro de 2023;

DECLARANDO que a violação dos direitos à privacidade e à proteção de dados pessoais é uma violação dos direitos humanos e das liberdades fundamentais e limita total ou parcialmente aos titulares de dados o reconhecimento, gozo e exercício de tais direitos e liberdades e de outros direitos humanos;

PREOCUPADOS que a tecnologia da informação esteja ao serviço de cada cidadão, que o desenvolvimento da sociedade da informação se dê em um quadro de cooperação internacional e que nenhuma tecnologia viole direitos humanos nem a tutela de dados pessoais, e não constitua uma ofensa à dignidade humana;

PREOCUPADOS que, cada vez mais frequentes incidentes de segurança nos setores público e privado, ameaçam a segurança dos cidadãos na região e os impeçam de aproveitar adequadamente os benefícios do gover-

no eletrônico, dos serviços digitais e do desenvolvimento sustentável por meio da tecnologia da informação;

CONVENCIDOS de que aumentar o nível de proteção de dados pessoais é uma prioridade para a região e uma condição essencial para o desenvolvimento individual e social e também para sua plena e igualitária participação em todas as esferas da sociedade da informação,

ACORDARAM o seguinte:

Capítulo I - Âmbito de aplicação e definições

Artigo 1. Objetivos

1.1. Esta Convenção tem como objeto:

a) Estabelecer as regras para garantir o devido tratamento dos dados pessoais e proteger direitos dos titulares dessa informação.

b) Facilitar o fluxo de dados entre os Estados-Membros com a finalidade de contribuir para o crescimento social e econômico e para o desenvolvimento sustentável da região.

c) Promover o desenvolvimento de mecanismos para cooperação internacional entre as autoridades de supervisão dos Estados-membros, as autoridades de supervisão dos Estados não membros desta Convenção e as autoridades e entidades internacionais na matéria.

1.2. A proteção de dados pessoais baseia-se:

a. no respeito a privacidade reconhecido no art. 11 do Convenção Americana sobre Direitos Humanos;

b. no direito à autodeterminação informativa;

c. na liberdade de expressão, informação, comunicação e opinião;

d. na inviolabilidade da privacidade, da honra e da imagem;

e. no desenvolvimento e inovação econômica e tecnológica;

f. na livre iniciativa, livre concorrência e proteção do consumidor;

g. nos direitos humanos, no livre desenvolvimento personalidade, na dignidade e no exercício de cidadania por pessoas naturais.

Artigo 2. Definições

2.1. Para os efeitos desta Convenção deve-se entender:

a. **Anonimização**: a aplicação de medidas de qualquer natureza destinadas a prevenir a identificação ou reidentificação de uma pessoa física sem esforços desproporcionais;

b. **Consentimento**: manifestação de vontade livre, específica, inequívoca e informada do titular dos dados, através da qual aceita e autoriza o tratamento dos dados pessoais que lhe dizem respeito;

c. **Dados Pessoais**: qualquer informação relativa a uma pessoa física identificada ou identificável, expressa em forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica ou qualquer outra forma. Uma pessoa é considerada identificável quando é possível determinar direta ou indiretamente sua identidade, desde que isso não despenda prazo ou atividades desproporcionais.

d. **Dados pessoais sensíveis**: aqueles que se referem à esfera íntima de seu titular ou cuja utilização indevida possa dar origem a discriminação ou implique um risco grave para este. De modo enunciativo, são considerados dados pessoais sensíveis as informações que possam, entre outros, revelar aspectos como origem racial ou étnica; crenças ou convicções religiosas, filosóficas e morais; filiação sindical; opiniões políticas; dados relativos à saúde, vida, preferência ou orientação sexual, dados genéticos ou dados biométricos destinados a identificar de forma única uma pessoa física.

e. **Operador:** prestador de serviços, que, como pessoa física ou jurídica ou autoridade pública, sem relação com a organização do controlador, processa dados pessoais em nome e por conta do deste último.

f. **Exportador**: pessoa física ou jurídica de direito privado, autoridade pública, serviço, organização ou prestador de serviços localizado em território de um Estado que realize transferências internacionais de dados pessoais, de acordo com o disposto nestas Normas.

g. **Controlador**: pessoa física ou jurídica privada, autoridade pública, serviço ou órgão que, isoladamente ou em conjunto com outros, determina os fins, meios, escopo e demais questões relacionadas ao tratamento de dados pessoais.

h. **Titular dos dados pessoais:** pessoa física a quem se referem os dados pessoais.

i. **Tratamento:** qualquer operação ou conjunto de operações realizado através de procedimentos físicos ou automatizados realizados com dados pessoais, relacionados, de modo enunciativo, mas não limitativo, com a obtenção, acesso, registro, organização, estruturação, adaptação, indexação, modificação, extração, consulta, armazenamento, conservação, elaboração, transferência, divulgação, posse, aproveitamento, e, em geral, qualquer uso ou disposição de dados pessoais.

Artigo 3. Âmbito de aplicação subjetivo

3.1. As obrigações e direitos estabelecidos nesta Convenção serão aplicáveis às pessoas físicas, autoridades e órgãos públicos que tratem dados pessoais no exercício de suas atividades e funções.

3.2. As obrigações e direitos estabelecidos nesta Convenção serão aplicáveis aos tratamentos de dados pessoais que estejam em suportes físicos ou, total ou parcialmente automatizados, ou em ambos os suportes, com independência da forma ou modalidade de sua criação, tipo de suporte, tratamento, armazenamento e organização.

3.3. As obrigações e direitos estabelecidos nesta Convenção serão aplicáveis aos dados pessoais de pessoas naturais, o que não impede que os Estados-Membros disponham em sua legislação nacional que as informações de pessoas jurídicas possam ser protegidas de acordo com o direito de proteção de dados pessoais, em conformidade com o estabelecido em seu direito interno.

3.4. As obrigações e direitos estabelecido nesta Convenção não serão aplicáveis nas seguintes situações:

a. Quando os dados pessoais se destinem exclusivamente a atividades internas em um contexto de vida familiar ou doméstica de uma pessoa física, ou seja, a utilização de dados pessoal em ambiente de amizade, parentesco ou grupo pessoal próximo e que não tenham como finalidade a divulgação ou utilização comercial dos referidos dados.

b. A informação anônima em sua origem, isto é, aquela que não guarda relação com uma pessoa física identificada ou identificável, bem como dados pessoais submetidos a um processo de anonimização, de tal forma que o titular não possa ser identificado ou reidentificado.

Artigo 4. Âmbito de aplicação territorial

4.1. Os direitos reconhecidos nesta Convenção serão aplicáveis ao tratamento de dados pessoais realizado:

a. Por um controlador ou operador estabelecido em território dos Estados-Membros.

b. Por um controlador ou operador não estabelecido em território dos Estados-Membros, quando as atividades de tratamento estejam relacionadas à oferta de bens ou serviços destinados aos residentes dos Estados-Membros, ou que estejam relacionados com o controle de seu comportamento, na medida em que isto ocorra nos Estados-Membros.

c. Por um controlador ou operador que não esteja estabelecido em um dos Estados-Membros, mas que esteja sujeito à aplicação de uma legislação nacional de um desses Estados, derivada da celebração de um contrato ou em virtude de princípios de Direito internacional público.

d. Por um controlador ou operador não estabelecido em território de qualquer dos Estados-Membros, e que utilize ou recorra a meios, automatizados ou não, localizados nesse território para tratar dados pessoais, a menos que estes meios sejam usados apenas para fins de trânsito.

4.2. Para os efeitos desta Convenção, estabelecimento significará o local de administração central ou principal do controlador ou operador, que deverá ser determinado com base em critérios objetivos e implicar o exercício efetivo e real de atividades de gestão que determinem as principais decisões em relação aos fins e meios do tratamento de dados pessoais que realize, com natureza estável e permanente.

4.3. A presença e utilização de meios técnicos e tecnologias para o tratamento de dados pessoais ou atividades de tratamento não constituirão, em si mesmas, um estabelecimento principal e não serão considerados como critérios determinantes para a definição do estabelecimento principal do controlador ou operador.

Capítulo II - Princípios aplicáveis ao tratamento de dados pessoais

Artigo 5. Princípio da dignidade humana

Os Estados adotarão medidas necessárias e eficazes, inclusive de ordem legislativa, para garantir que todos os desenvolvimentos científicos ou tecnológicos sejam em benefício da dignidade humana, dos direitos humanos, das liberdades fundamentais, da sociedade e da humanidade.

Artigo 6. Princípio da legitimação

6.1. Como regra geral, o Controlador apenas poderá tratar dados pessoais quando estiver presente alguma destas hipóteses:

a. O titular outorgue seu consentimento expresso para uma ou várias finalidades específicas.

b. O tratamento seja necessário para cumprimento de ordem judicial, resolução ou mandado fundamentado e motivado de autoridade pública competente.

c. O tratamento seja necessário para exercício das faculdades próprias das autoridades públicas, ou seja, realizado em virtude de autorização legal.

d. O tratamento seja necessário para o reconhecimento ou defesa dos direitos do titular perante uma autoridade pública.

e. O tratamento seja necessário para a execução de um contrato ou pré-contrato do qual o titular seja parte.

f. O tratamento seja necessário para o cumprimento de uma obrigação legal aplicável ao controlador.

g. O tratamento seja necessário para proteger interesses vitais do titular ou de outra pessoa física.

h. O tratamento seja necessário por razões de interesse público estabelecidas ou previstas em lei.

i. O tratamento seja necessário para a satisfação dos interesses legítimos perseguidos pelo controlador ou por um terceiro, desde que os referidos interesses não prevaleçam sobre os interesses ou direitos e liberdades fundamentais do titular que requeira a proteção de dados pessoais, especialmente quando o titular seja criança ou adolescente. O acima exposto

não será aplicável aos tratamentos de dados pessoais realizados por autoridades públicas no exercício de suas funções legais.

Artigo 7. Princípio do consentimento

7.1. Quando for necessária a obtenção do consentimento do titular, o controlador demonstrará de maneira inequívoca que o titular concedeu seu consentimento, seja através de uma declaração ou de uma ação afirmativa clara.

7.2. Sempre que seja necessário o consentimento para o tratamento dos dados pessoais, o titular poderá revogá-lo a qualquer momento, por meio de mecanismos simples, ágeis, eficazes e gratuitos estabelecidos pelo controlador.

Artigo 8. Consentimento para tratamento de dados relacionados a crianças ou adolescentes

8.1. Na obtenção do consentimento de crianças ou adolescentes, o controlador deverá obter a autorização do detentor do poder familiar ou de tutela do menor, de acordo com disposto em as regras de representação previstas no direito interno dos Estados-membros, ou, caso seja possível, solicitar diretamente a autorização ao menor se o direito interno de cada Estado-Membro estabelecer uma idade mínima para que o menor possa concedê-lo diretamente e sem representação do detentor de poder familiar ou tutela.

8.2. O controlador deverá, considerando a tecnologia disponível, empreender esforços razoáveis para verificar que o consentimento foi outorgado pelo detentor do poder familiar ou da tutela, ou pelo menor diretamente com base na sua idade, de acordo com direito interno de cada Estado-membro.

8.3. Os tratamentos de dados pessoais de crianças ou adolescentes devem ser realizados em seu melhor interesse, de acordo com o artigo 21 desta Convenção.

Artigo 9. Princípio da legalidade

9.1. O controlador tratará os dados pessoais em sua posse com a estrita observância e cumprimento do disposto no direito interno do Estado-Membro que resulte aplicável, do direito internacional e dos direitos e liberdades das pessoas.

9.2. O tratamento de dados pessoais realizado por autoridades públicas estará sujeito a faculdades ou atribuições conferidas expressamente pelo direito interno do Estado-Membro em questão, além do que está previsto no artigo anterior desta Convenção.

Artigo 10. Princípio da lealdade e boa fé

10.1. O controlador ou operador do tratamento deverão agir no pleno respeito do princípio da boa-fé. Neste sentido, o controlador tratará os dados pessoais em sua posse privilegiando a proteção dos interesses do titular e abstendo-se de tratá-los por meios enganosos ou fraudulentos.

10.2. Para os efeitos desta Convenção, serão considerados desleais aqueles tratamentos de dados pessoais que deem origem a uma discriminação injusta ou arbitrária contra os titulares.

Artigo 11. Princípio da transparência

11.1. O controlador informará ao titular sobre a existência e principais características dos tratamentos a que serão submetidos seus dados pessoais, visando possibilitar a tomada de decisões informadas a respeito.

11.2. O controlador fornecerá ao titular, pelo menos, as seguintes informações:

a. Sua identidade e dados para contato;

b. As finalidades do tratamento a que serão submetidos os seus dados pessoais;

c. As comunicações, nacionais ou internacionais, de dados pessoais que pretenda realizar, incluindo os destinatários e as finalidades que motivam a realização das mesmas.

d. A existência, forma e mecanismos ou procedimentos por meio dos quais será possível o exercício dos direitos definidos pelo artigo 20 desta Convenção.

e. Se for o caso, a origem dos dados pessoais quando o controlador não os tenha coletado diretamente do titular.

11.3. As informações fornecidas ao titular devem ser suficientes e facilmente acessíveis, bem como escritas e estruturadas em linguagem clara, simples e de fácil compreensão para os titulares aos quais sejam dirigidas, especialmente quando se tratar de crianças ou adolescentes.

11.4. Todo controlador deverá ter políticas transparentes sobre os tratamentos de dados pessoais que realize.

Artigo 12. Princípio da finalidade

12.1. Todo o tratamento de dados pessoais será limitado ao cumprimento de finalidades específicas, explícitas e legítimas.

12.2. O controlador não poderá tratar os dados pessoais em sua posse para fins distintos daqueles que motivaram seu tratamento original, a menos que haja alguma das causas que permita um novo tratamento de dados em acordo com o princípio da legitimação.

12.3. Os tratamentos ulteriores de dados pessoais para fins arquivísticos, de investigação científica e histórica ou para fins estatísticos, todos estes, em prol do interesse público, não serão considerados incompatíveis com as finalidades iniciais.

Artigo 13. Princípio da minimização

13.1. O controlador somente tratará dados pessoais que resultem adequados, pertinentes e limitados ao mínimo necessário em relação aos fins que justifiquem seu tratamento.

Artigo 14. Princípio de qualidade

14.1. O controlador adotará as medidas necessárias para manter a precisão, completude e atualização dos dados pessoais em sua posse, de tal forma que não se altere sua veracidade, conforme exigido para o cumprimento das finalidades que motivaram o tratamento. A informação sujeita ao tratamento deve ser verdadeira, completa, exata, atualizada e verificável. É proibido o tratamento de dados parciais, incompletos, fragmentados ou que induzam a erro.

14.2. Quando os dados pessoais deixarem de ser necessários para cumprimento das finalidades que motivaram seu tratamento, o controlador irá excluí-los ou eliminá-los de seus arquivos, registros, bancos de dados ou sistemas de informação, ou, se for o caso, irá submetê-los a um processo de anonimização.

14.3. No processo de exclusão dos dados pessoais, o controlador implementará métodos e técnicas visando a eliminação definitiva e segura destes.

14.4. Os dados pessoais apenas deverão ser conservados durante o prazo necessário para o cumprimento das finalidades que justifiquem seu tratamento ou aquelas relacionadas a requisitos legais aplicáveis ao controlador. Não obstante, a legislação nacional dos Estados-Membros poderá estabelecer exceções quanto ao período de conservação dos dados pessoais, respeitados os direitos e garantias do titular.

Artigo 15. Princípio da responsabilidade comprovada

15.1. O controlador implementará os mecanismos úteis, pertinentes, eficazes e oportunos que sejam necessários para comprovar a conformidade com os princípios e obrigações estabelecidos nesta Convenção, bem como prestará contas sobre os tratamentos de dados pessoais em sua posse ao titular e à autoridade de controle, podendo, para tanto, valer-se de padrões técnicos, melhores práticas nacionais ou internacionais, sistemas de autorregulação, sistemas de certificação ou qualquer outro mecanismo que determine ser apropriado para tais fins.

15.2. O artigo anterior será aplicado quando os dados pessoais forem tratados por um operador em nome e por conta do controlador, bem como no momento de realizar transferências de dados pessoal.

15.3. Entre os mecanismos que o controlador pode adotar para cumprir com o princípio da responsabilidade comprovada estão, de modo enunciativo, mas não limitativo, os seguintes:

a. Alocar recursos para implementação de programas e políticas de proteção de dados pessoais;

b. Implementar sistemas de gestão de riscos associado ao tratamento de dados pessoais;

c. Desenvolver políticas e programas de proteção de dados pessoais obrigatórios e exigíveis dentro da organização do controlador;

d. Colocar em prática um programa de capacitação e atualização de pessoal sobre as obrigações relacionadas à proteção de dados pessoais;

e. Revisar periodicamente políticas e programas de segurança de dados pessoais para determinar as modificações que forem necessárias;

f. Estabelecer um sistema de supervisão e vigilância interno e/ou externo, incluindo auditorias, para verificar a conformidade com políticas de proteção de dados pessoais;

g. Estabelecer procedimentos para receber e responder às dúvidas e reclamações de titulares.

15.4. O controlador deverá revisar e avaliar permanentemente os mecanismos que adotar voluntariamente para o efeito de cumprimento do princípio da responsabilidade comprovada, com a finalidade de mensurar seu nível de eficácia em relação ao cumprimento da legislação nacional aplicável.

Artigo 16. Princípio da segurança

16.1. O responsável estabelecerá e manterá, independentemente do tipo de tratamento que efetue, medidas de caráter administrativo, humano, contratual, físico, técnico e de qualquer outra natureza que sejam suficientes para, de um lado, garantir a segurança, confidencialidade, integridade e disponibilidade dos dados pessoais e, por outro lado, evitar a perda, manipulação, consulta, uso ou acesso não autorizado ou fraudulento de suas informações.

No caso de dados pessoais sensíveis e de crianças ou adolescentes, implementará medidas mais estritas para garantir a segurança e confidencialidade da informação (segurança reforçada).

16.2. Para a determinação das medidas referidas no inciso anterior, o controlador considerará os seguintes fatores:

a. O risco para direitos e liberdades dos titulares, em particular, devido ao potencial valor quantitativo e qualitativo que poderiam ter os dados pessoais tratados por um terceiro não autorizado à sua posse;

b. O estado atual da técnica;

c. Custos de implementação;

d. A natureza dos dados pessoais tratados, especialmente quando envolver dados pessoais sensíveis;

e. O escopo, o contexto e as finalidades do tratamento;

f. As transferências internacionais de dados pessoais que serão realizadas ou que se pretendam realizar;

g. O número de titulares envolvidos;

h. As possíveis consequências para os titulares que poderiam surgir de uma violação;

i. As violações anteriores que ocorreram no tratamento de dados pessoais.

16.3. O controlador realizará uma série de ações que garantirão o estabelecimento, implementação, operação, monitoramento, revisão, manutenção e melhoria contínua das medidas de segurança aplicáveis ao tratamento de dados pessoais periodicamente.

Artigo 17. Notificação de violações à segurança dos dados pessoais

17.1. Quando o controlador tiver conhecimento de uma violação à segurança de dados pessoais ocorrido em qualquer fase de tratamento, entendida como qualquer dano, perda, alteração, destruição, acesso e, em geral, qualquer uso ilícito ou não autorizado de dados pessoais, ainda quando ocorrerem de uma maneira acidental, deverá notificar a autoridade de controle e os titulares afetados pelo evento, sem qualquer atraso.

17.2. Adicionalmente, deverá adotar as medidas necessárias para evitar que qualquer incidente de segurança cause danos aos titulares dos dados, ou que, dependendo do caso, o mesmo seja o mínimo possível.

17.3. O inciso anterior não será aplicável quando o controlador puder demonstrar, tendo em vista o princípio da responsabilidade proativa, a improbabilidade da violação de segurança ocorrida, ou que esta não representa um risco aos direitos e liberdades dos titulares envolvidos.

17.4. A notificação realizada pelo controlador aos titulares afetados será redigida em linguagem clara e simples.

17.5. A notificação a que se referem os incisos anteriores conterão, pelo menos, as seguintes informações:

a. A natureza do incidente;

b. Os dados pessoais comprometidos;

c. As medidas corretivas imediatamente realizadas;

d. As recomendações ao titular sobre as medidas que este possa adotar para proteger os seus interesses;

e. Os meios disponíveis ao titular para obter maiores informações a respeito.

17.6. O controlador documentará qualquer violação de segurança aos dados pessoais ocorrida em qualquer fase de tratamento, identificando, mas

não se limitando, à data em que ocorreu; o motivo da violação; os fatos relacionados e seus efeitos e também as medidas corretivas implementadas imediata e definitivamente, o que deverá estar disponível para autoridade de controle.

17.7. A legislação nacional dos Estados-Parte aplicável à matéria estabelecerá os efeitos das notificações de violações de segurança feitas pelo controlador às autoridades de controle no que se refere a procedimentos, forma e condições da sua intervenção, com a finalidade de salvaguardar interesses, direitos e liberdades dos titulares afetados.

Artigo 18. Princípio da confidencialidade

18.1. O controlador estabelecerá controles ou mecanismos para que quaisquer intervenientes, em qualquer fase de tratamento dos dados pessoais, mantenham e respeitem a confidencialidade dos mesmos, uma obrigação que subsistirá mesmo após o término seu relacionamento com o titular.

Artigo 19. Princípio da prevenção e precaução

19.1. Os Controladores e Operadores do tratamento de dados pessoais deverão implementar medidas preventivas para evitar danos ou prejuízos aos titulares de dados, ou vulnerar seus direitos. Quando o tratamento de dados pessoais for susceptível de causar danos graves e irreversíveis, o controlador ou operador deverá se abster de realizar o tratamento ou adotar medidas de precaução ou preventivas para proteger os direitos do titular dos dados, sua dignidade humana e outros direitos humanos.

19.2. Da mesma forma, o Controlador ou Operador do tratamento deverá abster-se de realizar o referido tratamento ou adotar medidas adequadas para proteger os direitos do titular ou titulares dos dados, a sua dignidade humana e outros direitos humanos com base no princípio da precaução. Esse princípio também se aplica quando o risco ou magnitude do dano produzido ou que possa ocorrer não são previstos, por não existir forma de estabelecer, a médio ou longo prazo, os efeitos de um tratamento de dados.

19.3 Para identificar riscos, o Controlador e o Operador devem realizar uma avaliação de impacto preliminar e, idealmente, testar as atividades de tratamento propostas em ambientes controlados para experimentação e inovação, como sandboxes.

Capítulo III - Dos direitos protegidos

Artigo 20. Direito à autodeterminação informativa e proteção de dados pessoais

20.1. Toda pessoa tem direito à autodeterminação informativa e à proteção dos seus dados pessoais em conformidade com as regras desta Convenção. Ditos direitos são concretizados com a faculdade de cada pessoa exercer controle sobre seus dados pessoais, que serão tratados de forma lícita, legítima, leal, transparente, segura, responsável e confidencial, para fins explicitamente definidos com base no consentimento da pessoa afetada ou em virtude de outra base legítima prevista pela lei.

20.2. A todas as pessoas cujos dados sejam tratados serão garantidos os direitos definidos pelo artigo 21 desta Convenção. As autoridades reguladoras independentes designadas por cada Estado-Membro serão responsáveis por garantir total respeito a estes direitos.

Artigo 21. Direitos

21.1. Toda pessoa terá direito a:

a. não estar sujeita a uma decisão que a afete significativamente, baseada apenas em um tratamento automatizado de dados sem considerar suas opiniões. Esta regra não será aplicável se a decisão foi autorizada por lei a qual o controlador está sujeito e quando esta lei estabelecer medidas adequadas para garantir direitos, liberdades e interesses legítimos do titular dos dados;

b. obter, quando assim o solicitar, em intervalos razoáveis e sem demora ou despesas excessivas, a confirmação do tratamento dos dados pessoais relacionados à sua pessoa, a comunicação de forma inteligível dos dados tratados, todas as informações disponíveis sobre sua origem, o período de conservação, bem como qualquer outra informação que o controlador deva fornecer a fim de garantir a transparência do tratamento, incluindo as medidas de segurança adotadas sobre seus dados pessoais;

c. obter, quando assim o solicitar, conhecimento da fundamentação subjacente ao tratamento dos dados quando os resultados do referido tratamento se lhe aplicarem;

d. opor-se a qualquer momento, por motivos relacionados à sua situação, ao tratamento de dados pessoal que lhe envolva, a menos que controlador demonstre fundamentos legítimos para o tratamento superiores aos seus interesses, direitos ou liberdades fundamentais;

e. obter, quando assim o solicitar, sem custos e sem demoras excessivas, a retificação ou eliminação, conforme o caso, dos referidos dados se estes foram ou estiveram sendo tratados de maneira contrária às disposições desta Convenção;

f. obter uma solução jurídica de acordo com o que está previsto Artigo 26 desta Convenção quando seus direitos de conformidade com esta forem violados;

g. beneficiar-se, qualquer que seja sua nacionalidade ou residência, da assistência de uma autoridade supervisora de acordo com o disposto no Artigo 27 desta Convenção, para exercer seus direitos em conformidade à presente Convenção;

h. quando houver tratamento de dados pessoais por meio eletrônico ou automatizado, o titular terá direito a obter uma cópia dos dados pessoais que tenham sido fornecidos ao controlador ou que sejam objeto de tratamento, em um formato eletrônico estruturado, de uso comum e leitura mecânica, que permita continuar utilizando-os e transferi-los para outro controlador, nos casos em que exigir;

i. quando houver tratamento de dados pessoais por meio eletrônico ou automatizado, o titular terá direito de solicitar a revisão de decisões tomadas exclusivamente com base no tratamento automatizado de dados que afetam seus interesses, incluindo as decisões que visam definir o seu perfil pessoal, profissional, de consumo e de crédito ou aspectos de sua personalidade. Consequentemente, o controlador deverá fornecer, quando solicitado, informações claras e adequadas sobre os critérios e procedimentos utilizados para a decisão automatizada, observados os segredos comerciais e industriais.

j. os Estados-Membros deverão adotar, sempre que possível, o direito à revisão por pessoa humana das decisões automatizadas.

21.2. O titular poderá solicitar que seus dados pessoais sejam transferidos diretamente de um controlador para outro controlador, quando for tecnicamente possível. O direito à portabilidade de dados pessoais não afetará negativamente os direitos e liberdades de outrem.

21.3. Sem prejuízo aos outros direitos do titular, o direito à portabilidade de dados pessoais não procederá quando se tratar de informações inferidas, derivadas, criadas, geradas ou obtidas a partir da análise ou tratamento realizado pelo controlador com base nos dados pessoais fornecidos pelo titular, como é o caso dos dados pessoais que tenham sido submetidos a um tratamento de personalização, recomendação, categorização ou criação de perfil.

21.4. Os Estados-Membros deverão conceder a todas as pessoas recursos judiciais eficazes para a proteção dos direitos reconhecidos nesta Convenção, incluindo a indenização por tratamento não autorizado de dados pessoais ou violação de direitos reconhecida.

21.5. A legislação nacional dos Estados-Membros aplicável reconhecerá o direito do titular a ser indenizado quando houver sofrido danos e prejuízos, como consequência de uma violação de seu direito de proteção aos dados pessoais.

21.6. O direito interno dos Estados-Membros indicará a autoridade competente para conhecer este tipo de ação interposta pelo titular afetado, bem como os prazos, requisitos e condições por meio dos quais será indenizado em caso de procedência.

Artigo 22. Tratamento de dados pessoais de crianças ou adolescentes

22.1. No tratamento de dados pessoais relativos às crianças ou adolescentes, os Estados- Membros da Convenção deverão privilegiar a proteção de seu melhor interesse, em conformidade com a Convenção sobre Direitos da Criança e outros instrumentos internacionais que buscam seu bem-estar e proteção abrangente.

22.2. Estados-Membros promoverão, na formação acadêmica de crianças e adolescentes, o uso responsável, adequado e seguro de tecnologias da informação e comunicação e eventuais riscos que possam enfrentar em ambientes digitais relacionados ao tratamento indevido de seus dados pessoais, bem como o respeito pelos seus direitos e liberdades.

Artigo 23. Tratamento de dados pessoais sensíveis

23.1. Como regra geral, o controlador não poderá tratar dados pessoais sensíveis, exceto quando atender a qualquer um destes requisitos:

a. Os mesmos sejam estritamente necessários para o exercício e cumprimento de poderes e obrigações expressamente previstos nas normas que regulem sua atuação.

b. Para cumprimento de ordem legal.

c. Por meio do consentimento expresso e por escrito do titular.

d. Caso sejam necessários por razões de segurança nacional, segurança pública, ordem pública, saúde pública ou salvaguarda dos direitos e liberdades de terceiros.

23.2. A legislação nacional dos Estados-Membros aplicável à matéria poderá estabelecer exceções, garantias e condições adicionais para garantir o devido tratamento de dados pessoais sensíveis, de acordo com seu direito interno.

Artigo 24. Exceções e restrições

24.1. Nenhuma exceção será permitida às disposições estabelecidas neste Capítulo, salvo se dita exceção se encontre prevista em lei, respeite a essência de direitos consagrados nesta Convenção e também as liberdades fundamentais, além de constituir uma medida necessária e proporcional numa sociedade democrática para:

a. proteção da segurança nacional, defesa, segurança pública, importantes interesses econômicos e financeiros do Estado, a imparcialidade e independência do Poder Judiciário ou da prevenção, investigação e repressão de crimes, bem como a aplicação de sanções penais e outros objetivos essenciais de interesse público geral;

b. proteger o titular dos dados ou direitos e liberdades fundamentos de outros, em particular, a liberdade de expressão.

24.2. As restrições para o exercício das disposições especificadas nos artigos 18 e 19 devem ser previstas por lei, com respeito ao tratamento de dados com a finalidade de arquivo no interesse público, investigação científica ou histórica ou finalidades estatísticas, quando não haja risco identificável de violação dos direitos e das liberdades fundamentais dos titulares de dados.

24.3. As atividades de tratamento para fins de segurança e defesa nacional estão sujeitas a revisão e supervisão independente e efetiva, de acordo com as leis locais do Estado-Parte pertinente.

Capítulo IV - Das obrigações

Artigo 25. Obrigações

25.1. Cada Estado-Parte deverá providenciar que os controladores e, se for o caso, os operadores, tomem todas as medidas necessárias para cumprir com as obrigações desta Convenção e sejam capazes de demonstrar, sujeito às leis locais, que o tratamento de dados sob seu controle cumpre com as disposições desta Convenção.

25.2. Cada Estado-Parte deverá providenciar que os controladores e, se for o caso, os operadores, examinem o impacto provável de tratamento de dados sobre direitos e liberdades fundamentais dos titulares dos dados, previamente ao início do referido tratamento, e deverão projetar o tratamento de forma a prevenir ou minimizar o risco de interferência em direitos ou liberdades fundamentais.

25.3. Cada Estado-Parte deverá providenciar que os controladores e, se for o caso, os operadores, implementem medidas técnicas e organizacionais que levem em conta as implicações do direito de proteção de dados pessoais em todas as etapas do tratamento de dados.

25.4. Cada Estado-Parte poderá, considerando os riscos em relação aos interesses, direitos e liberdades fundamentais dos titulares dos dados, adaptar a aplicação das disposições dos parágrafos 1, 2 e 3 na lei que torne eficaz as disposições desta Convenção, de acordo com a natureza e o volume dos dados, a natureza, escopo e finalidade do tratamento e, se for o caso, o tamanho controlador ou do operador.

Capítulo V – Transferência e coleta internacional de dados pessoais

Artigo 26. Regras gerais para transferências de dados pessoais

26.1. O controlador e o operador poderão fazer transferências internacionais de dados pessoais em qualquer uma das seguintes hipóteses:

a. O país, parte de seu território, setor, atividade ou organização internacional destinatário dos dados pessoais tiver sido reconhecido com um nível de proteção de dados adequada pelo país exportador, de acordo com a legislação nacional deste que resulte aplicável, ou seja o país destinatário ou vários setores do mesmo demonstrem condições mínimas e suficientes para garantir um nível de proteção de dados pessoais adequado, sendo o respeito às disposições desta Convenção considerado como garantia de tais condições mínimas e suficientes.

b. O exportador ofereça garantias suficientes de tratamento dos dados pessoais no país destinatário, e isso, por sua vez, demonstre o cumprimento das condições mínimas e suficientes estabelecidas na legislação nacional de cada Estado-Membro aplicável à matéria.

c. O exportador e o destinatário assinem cláusulas contratuais ou qualquer outro instrumento jurídico que ofereça garantias suficientes e que permita demonstrar o alcance do tratamento dos dados pessoais, as obrigações e responsabilidades assumidas pelas partes e pelos direitos dos titulares. A autoridade supervisora poderá validar cláusulas contratuais ou instrumentos legais conforme determinado em legislação nacional dos Estados aplicáveis à matéria.

d. O exportador e o destinatário adotem um esquema de códigos corporativos vinculantes ou um mecanismo de certificação aprovado, desde que esteja de acordo com as disposições previstas em legislação nacional do Estado-Membro aplicável à matéria, a qual o exportador está obrigado a observar.

e. A autoridade supervisora do Estado-Membro do país do exportador autorize a transferência, nos termos de legislação nacional aplicável à matéria.

26.2. A legislação nacional dos Estados-Membros aplicável será capaz de estabelecer expressamente os limites para transferências internacionais

de categorias de dados pessoais por razões de segurança nacional, segurança pública, proteção da saúde pública, proteção de direitos e liberdades de terceiros, bem como para assuntos de interesse público.

Artigo 27. Coleta internacional de dados pessoais

27.1. Os Estados adotarão medidas adequadas, úteis e oportunas para garantir o tratamento adequado dos dados pessoais e a proteção efetiva dos direitos das pessoas cujas informações são coletadas de terceiros países por controladores ou operadores localizados em países diferentes do seu domicílio ou residência do titular dos dados pessoais e que não possuam sede física ou estabelecimento no mesmo (coletor de dados internacional).

27.2. Além disso, os Estados cooperarão entre si, com as autoridades de proteção de dados e com os titulares dos dados para garantir o objetivo indicado no parágrafo anterior.

27.3. A não presença, residência física ou estabelecimento do coletor internacional de dados no país do titular dos dados não poderá ser uma excusa para o descumprimento das obrigações ou falta de proteção dos direitos definidos nesta Convenção.

Capítulo VI - Das autoridades de controle

Artigo 28. Natureza das autoridades de controle e supervisão

28.1. Em cada Estado-Membro deve existir uma ou mais autoridades de controle em matéria de proteção de dados pessoais com total autonomia, de acordo sua legislação nacional aplicável.

28.2. As autoridades de controle poderão ser órgãos individuais ou pluripessoais; agirão de forma imparcial e independente em seus poderes, assim como serão alheios a toda influência externa, seja direta ou indireta, e não solicitarão ou admitirão ordem ou instrução alguma.

28.3. O membro ou membros de órgãos de gestão das autoridades de controle devem ter experiência e competências, em particular no que

diz respeito ao domínio da proteção de dados pessoais, necessários para o cumprimento dos seus deveres e exercício dos seus poderes. Seus funcionários serão nomeados por um procedimento transparente em virtude de legislação nacional aplicável e apenas poderão ser removidos por motivos graves comprovados no direito interno de cada Estado-Membro, de acordo com as regras do devido processo.

28.4. A legislação nacional dos Estados-Membros que aplicável à matéria deverá conceder às autoridades de supervisão poderes suficientes de investigação, supervisão, auditoria, resolução, promoção, sanção e outros que possam ser necessários para garantir seu efetivo cumprimento, bem como o exercício e respeito do direito à proteção de dados pessoais.

28.5. As decisões das autoridades de supervisão estarão sujeitas a controle somente jurisdicional, de acordo com os mecanismos estabelecidos na legislação nacional dos Estados-Membros aplicável em seu direito interno.

28.6. As autoridades de controle deverão contar com recursos humanos e materiais necessários para o cumprimento de suas funções.

Artigo 29. Regime de reclamações e aplicação de sanções

29.1. Cada titular terá direito de apresentar a sua reclamação perante a autoridade de controle, bem como recorrer à proteção judicial para efetivar seus direitos ao abrigo da legislação nacional do Estado-Membro aplicável, incluindo o pedido de cessação de conduta violadora da Convenção, medidas cautelares para impedir danos e compensação dos prejuízos de qualquer natureza causados pelo tratamento ilegal de dados pessoais.

29.2. A legislação nacional dos Estados-Membros aplicável estabelecerá um regime que permita ao titular apresentar uma reclamação perante a autoridade de supervisão quando considerar que o tratamento de seus dados pessoais infrinja normas nacionais sobre a matéria, bem como solicitar tutelas judiciais.

29.3. A legislação nacional dos Estados-Membros aplicável estabelecerá um regime que permita a adoção de medidas corretivas e sanções a comportamentos que contrariem o disposto nas legislações nacionais correspondentes, indicando, pelo menos, o limite máximo e critérios objetivos para

definir as sanções correspondentes, desde a natureza, gravidade, duração da infração e suas consequências, bem como as medidas implementadas pelo controlador para garantir o cumprimento de suas obrigações na matéria.

Capítulo VII - Mecanismos de proteção interamericana

Artigo 30. Comissão Interamericana de Proteção de Dados Pessoais

30.1. A Comissão Interamericana de Proteção de Dados pessoais funcionará como um órgão autônomo e será responsável pela promoção e proteção de direitos reconhecidos nesta Convenção nos países membros. Será composta pelas autoridades de proteção de dados dos países membros da Convenção, que atuarão *ad honorem*.

30.2. A Comissão Interamericana de Proteção de Dados Pessoais adotará seu próprio regimento interno.

30.3. A Comissão Interamericana de Proteção de Dados Pessoais terá uma Secretaria Geral que terá caráter administrativo do Convênio e será exercida de forma rotativa e pelo prazo de dois anos por alguma das autoridades de proteção de dados dos países membros da Convenção. Inicialmente, a Secretaria Geral estará a cargo da autoridade de proteção de dados do primeiro Estado-membro que ratifique o Convênio e o notifique aos outros Estados signatários.

30.4. A função de Secretário Geral da Comissão Interamericana de Proteção de Dados Pessoais é exercida, de maneira rotativa e pelo prazo de dois anos, pelo presidente da mesma autoridade que exerça a Secretaria Geral rotativa.

30.5. Suas funções serão:

a. facilitar a comunicação, a cooperação e a coordenação entre as autoridades nacionais de proteção de dados dos países membros;

b. elaborar um relatório anual sobre o estado da proteção de dados na região;

c. preparar documentos, pareceres e guias sobre a aplicação e interpretação da Convenção;

d. colaborar com os Estados-Membros na implementação deste tratado em suas leis locais, sem prejuízo das regras que resultem diretamente aplicáveis;

e. Receber os instrumentos de ratificação da Convenção e as propostas de modificação do mesmo.

Artigo 31. Relatórios

31.1. Com a finalidade de proteger o direito das pessoas à proteção dos seus dados pessoais, nos relatórios nacionais à Comissão Interamericana de Proteção de Dados Pessoais, os Estados-Partes deverão incluir informações sobre as medidas tomadas para prevenir e efetivar direitos reconhecidos nesta Convenção, bem como sobre as dificuldades que observarem na aplicação dos mesmos e os fatores que contribuam para a proteção adequada de dados pessoais.

Artigo 32. Pareceres consultivos

32.1. Os Estados-Partes nesta Convenção e as respectivas agências de proteção de dados pessoais poderão requerer à Comissão Interamericana de Proteção de Dados Pessoais um parecer consultivo sobre a interpretação desta Convenção.

Artigo 33. Recursos

33.1. Qualquer pessoa ou grupo de pessoas, ou entidade não governamental legalmente reconhecida em um ou mais Estados-Membros da Organização, poderá apresentar petições à Comissão Interamericana de Proteção de Dados que contenham denúncias ou queixas de violação dos direitos previstos nesta Convenção por um Estado-Parte, e a Comissão as considerará de acordo com as regras e requisitos procedimentais para a apresentação e consideração de petições estipuladas em seu próprio regimento interno.

Capítulo VIII - Disposições gerais da convenção

Artigo 34

34.1. Nada do disposto na presente Convenção poderá ser interpretado como uma restrição ou limitação à legislação interna dos Estados-Partes que preveja iguais ou maiores proteções e garantias de direitos aos titulares de dados pessoais.

Artigo 35

35.1. Nada do disposto na presente Convenção pode ser interpretado como uma restrição ou limitação à Convenção Americana sobre Direitos Humanos ou outras convenções internacionais sobre matéria que proporcione igual ou maior proteções relacionadas a este tópico.

Artigo 36

36.1. Esta Convenção está aberta à assinatura de todos os estados do continente americano.

Artigo 37

37.1. Esta Convenção está sujeita a ratificação.
Artigo 38.
38.1. Esta Convenção está aberta à adesão de qualquer um outro estado.

Artigo 39

39.1. Os Estados não poderão formular reservas a esta Convenção no momento da sua aprovação, assinatura, ratificação ou adesão a ela.

Artigo 40

40.1. Qualquer Estado parte pode submeter, aos outros Estados-membros da Convenção uma proposta de emenda a esta Convenção. As alterações entrarão em vigor para os Estados que as ratificarem na data em

que dois terços dos Estados Partes tenham depositado o respectivo instrumento de ratificação. Quanto aos demais Estados Partes, entrarão em vigor na data em que depositarem os respectivos instrumentos de ratificação.

Artigo 41

41.1. Estados Partes que possuem duas ou mais unidades territoriais naqueles que regem diferentes sistemas jurídicos relacionados a assuntos discutidos na presente Convenção poderá declarar, no momento da assinatura, ratificação ou adesão, que a Convenção aplicar-se-á a todas as suas unidades territoriais ou apenas a uma ou mais delas. Tais declarações podem ser modificadas em qualquer momento por meio de declarações posteriores, que especificarão expressamente a unidade ou unidades territoriais às quais esta Convenção se aplicará.

Artigo 42

42.1. A presente Convenção entrará em vigor no trigésimo dia após a data em que o primeiro instrumento de ratificação tiver sido depositado. Para cada Estado que ratifique ou adira à Convenção após o depósito do segundo instrumento de ratificação, esta entrará em vigor no trigésimo dia a contar da data em que esse Estado tiver depositado o seu instrumento de ratificação ou de adesão.

Artigo 43

43.1. O Secretário-Geral informará a todos os Estados-Membros da Organização dos Estados Americanos a entrada em vigor desta Convenção**.**

Artigo 44

44.1. A Comissão Interamericana de Proteção de Dados Pessoais apresentará um relatório anual aos Estados-membros da Comissão Interamericana de Proteção de Dados Pessoais sobre o estado desta Convenção, incluindo assinaturas, depósitos de instrumentos de ratificação, adesão ou declarações, bem como as reservas apresentadas pelos Estados partes e, se for o caso, o relatório sobre as mesmas.

Artigo 45

45.1. Esta Convenção vigorará indefinidamente, mas qualquer dos Estados-Partes poderá denunciar esta Convenção mediante o depósito de um instrumento para esse fim na Secretária-geral da Comissão Interamericana de Proteção de Dados Pessoais. Um ano após a data do depósito do instrumento de denúncia, a Convenção cessará em seus efeitos para o Estado denunciante, permanecendo subsistente para os outros Estados-Partes.

Artigo 46

46.1. O instrumento original da presente Convenção, cujos textos em espanhol, e português são igualmente autênticos, será depositado na Secretária-geral da Comissão Interamericana de Proteção de Dados Pessoais, que enviará cópia autenticada de seu texto para registro e publicação pela Secretaria das Nações Unidas, de acordo com Artigo 102 da Carta das Nações Unidas.

EM TESTEMUNHO DO QUE, os plenipotenciários abaixo-assinados, devidamente autorizados pelos seus respectivos governos, assinam este presente Acordo, que se chamará "Convenção Interamericana sobre Autodeterminação Informativa, Tratamento e Circulação de Dados Pessoais."

Conheça melhor a editora Lumen Juris

www.lumenjuris.com.br
@lumenjuriseditora
publique@lumenjuris.com.br

O rápido avanço das tecnologias digitais transformou a forma como os dados pessoais são coletados, tratados e transferidos através das fronteiras, apresentando oportunidades e desafios para indivíduos, empresas, pesquisadores e governos em todo o mundo. Este livro tem como objetivo proporcionar uma análise inicial do complexo, embora convergente, panorama das transferências de dados pessoais na América Latina, lançando luz sobre os desafios em evolução, as respostas regulatórias e as possíveis soluções compartilhadas que podem moldar este aspecto crucial da governança de dados em nível regional.

Este volume explora a importância das transferências internacionais de dados pessoais, que se manifesta em vários aspectos de nossas economias e sociedades, a partir da pesquisa e desenvolvimento até o comércio eletrônico e a implementação de sistemas de inteligência artificial. As transferências internacionais de dados pessoais também representam desafios em termos de privacidade e segurança da informação. Portanto, marcos regulatórios, instrumentos contratuais e acordos internacionais são necessários para garantir a proteção de dados pessoais e a privacidade dos indivíduos no contexto das transferências internacionais de dados.

Partindo de uma análise de alguns dos sistemas mais proeminentes do continente, o livro identifica soluções pragmáticas e apresenta algumas propostas ambiciosas sobre como a América Latina poderia construir seu futuro em termos de proteção de dados. Tais estratégias se tornam essenciais para concretizar o direito à autodeterminação informativa, reconhecido expressamente pela Corte Interamericana de Direitos Humanos, em outubro de 2023, como um direito humano autônomo de respeito e cumprimento obrigatórios no sistema interamericano de direitos humanos.

FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

Lumen Juris Direito | 35 anos

ISBN 978-85-519-3246-9
9 788551 932469