Universidade de Brasília – UnB
Faculdade de Direito

ANA VITÓRIA CAVALCANTE DE CARVALHO MARQUES

A RELAÇÃO ENTRE A LEI BRASILEIRA 13.709/18 E O ARCABOUÇO JURÍDICO PARA PROTEÇÃO DE DADOS PESSOAIS DO JAPÃO E DA COREIA DO SUL A PARTIR DO MODELO TLICS

Comparing Brazil, Japan and South Korea's legal framework on personal data through the lenses of the TLICS Model

Brasília
2021

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE DIREITO

A RELAÇÃO ENTRE A LEI BRASILEIRA 13.709/18 E O ARCABOUÇO JURÍDICO PARA PROTEÇÃO DE DADOS PESSOAIS DO JAPÃO E DA COREIA DO SUL A PARTIR DO MODELO TLICS

Autor: Ana Vitória Cavalcante de Carvalho Marques

Orientador: Prof. Dr. Márcio Iorio Aranha

Monografia apresentada como requisito parcial à obtenção do grau de Bacharel, no Programa de Graduação da Faculdade de Direito da Universidade de Brasília.

Brasília, ___ de _____ de ____.

FOLHA DE APROVAÇÃO

ANA VITÓRIA CAVALCANTE DE CARVALHO MARQUES

A relação entre a lei brasileira 13.709/18 e o arcabouço jurídico para proteção de dados pessoais do Japão e da Coreia do Sul a partir do modelo TLICS.

Monografia apresentada como requisito parcial à obtenção do grau de Bacharel, no Programa de Graduação da Faculdade de Direito da Universidade de Brasília, linha de pesquisa de *Transformações da Ordem Social e Econômica e Regulação*.

Aprovada em: ___ de _____ de _____.

BANCA EXAMINADORA

_____
Prof. Dr. Márcio Iorio Aranha
(Orientador – Presidente)

_____
Profª. Drª. Laura Schertel Ferreira Mendes
(Membro)

_____
Profª. Drª. Miriam Wimmer
(Membro)

_____
Prof. M.e. Fernando Feitosa
(Suplente)

Agradecimentos

Agradeço, primeiramente aos meus pais, Nilda e Tounai, por desde cedo me ensinarem que o meu valor está naquilo que não pode me ser tirado, o conhecimento. Muito obrigada por nunca medirem esforços para me oferecer toda a estrutura e apoio necessários para minha formação acadêmica e profissional. Aos dois, minha eterna admiração por terem feito tanto, com tamanho amor.

Agradeço ao meu marido, Iure, o companheiro da minha vida. São tantas as nossas lembranças nos corredores da faculdade e agora também durante a escrita desse trabalho. Obrigada pela parceria ao ler essa monografia com cuidado, tecer comentários enriquecedores e me dar todo o suporte necessário para concluí-la. Só você poderia tornar esse período tão leve.

Agradeço à minha irmã, Ana Luíza, minha melhor amiga desde sempre. Suas palavras de incentivo me permitiram ir mais longe.

Agradeço à minha avó, Zilda, pelo empenho incansável ao cuidar de mim e sem o qual não teria chegado aqui.

Agradeço aos meus amigos de faculdade, por tornarem esses anos alguns dos melhores da minha vida. Lembrarei sempre com carinho das conversas, das risadas, dos conselhos e do auxílio sempre presente.

Agradeço ao professor Márcio Iorio, a quem devo a inspiração para o tema desta monografia, pela excelência na orientação do trabalho. Muito obrigada pelas revisões sempre diligentes e comentários apurados.

Por fim, agradeço a Deus, que me deu a vida, por me sustentar com Sua graça todos os dias.

FICHA CATALOGRÁFICA

Utilizar este link, ou equivalente da Biblioteca Central, para gerar a Ficha e inseri-la aqui

REFERÊNCIA BIBLIOGRÁFICA

MARQUES, A. V. C. de C. (2021). A relação entre a lei brasileira 13.709/18 e o arcabouço jurídico para proteção de dados pessoais do Japão e da Coreia do Sul a partir do modelo TLICS. Monografia Final de Curso, Faculdade de Direito, Universidade de Brasília, Brasília, DF, 129 p.

Sumário

INTRODUÇÃO 15

CAPÍTULO 1: Desenvolvimento normativo do direito à proteção de dados pessoais e os indicadores de proteção presentes no Modelo TLICS 19

1.1. O desenvolvimento do direito à proteção de dados pessoais 19

1.1.1. A primeira geração de leis de proteção de dados pessoais 19

1.1.2. Segunda geração de leis de proteção de dados pessoais 21

1.1.3. Terceira geração de leis de proteção de dados pessoais 23

1.1.4. Quarta geração de leis de proteção de dados pessoais 26

1.2. O Modelo TLICS como indicador de proteção de dados pessoais ... 29

1.2.1. O Modelo TLICS e suas teorias de apoio 30

1.2.2. O modelo TLICS e seus indicadores para proteção de dados pessoais 37

CAPÍTULO 2: Aspectos convergentes e divergentes entre a Lei sobre a Proteção de Informações Pessoais do Japão e a Lei de Proteção de Informações Pessoais da Coreia do Sul 40

1. Questões preliminares 40

2. Aspectos convergentes e divergentes entre a APPI e a PIPA 41

2.1. Autoridade de proteção de dados 42

2.1.1. Autônoma/Independente 42

2.1.2. Apresentação Unitária 43

2.2. Titulares de Dados 44

2.2.1. Definição 44

2.2.2. Direito de ser informado 46

2.2.3. Direito de Acesso 46

2.2.4. Direito à Retificação 48

2.2.5. Direito ao Esquecimento ou Direito ao Apagamento 48

2.2.6. Direito à Revogação 51

2.2.7. Direito à Limitação do Tratamento 52

2.2.8. Direito de Portabilidade de Dados 54

2.2.9. Direito a Bloqueio ou Restrição do Processamento 54

2.2.10. Direito à Intervenção Humana na Tomada de Decisão e Criação de Perfil Automatizadas 56

2.2.11. Limitações 56

2.3. Transferência Internacional de Dados ou Processamento Transfronteiriço 58

2.3.1. Decisão de Adequação 58
2.3.2. Consentimento 59
2.3.3. Contrato 60
2.3.4. Regras Vinculativas Aplicáveis às Empresas 62
2.3.5. Certificados e Códigos de Conduta 63
3. Conclusões acerca das principais divergências e convergências entre a APPI e PIPA 64

CAPÍTULO 3: Aspectos convergentes e divergentes entre a Lei sobre a Proteção de Informações Pessoais do Brasil, do Japão e da Coreia do Sul . 66
1. Questões preliminares 66
2. Aspectos convergentes e divergentes entre a LGPD e a APPI 66
2.1. Autoridade de proteção de dados 66
2.1.1. Autônoma/Independente 67
2.1.2. Apresentação unitária 70
2.2. Titulares de Dados 70
2.2.1. Definição 70
2.2.2. Direito de ser informado 71
2.2.3. Direito de Acesso 72
2.2.4. Direito à Retificação 73
2.2.5. Direito ao Esquecimento ou Direito ao Apagamento 73
2.2.6. Direito à Revogação 74
2.2.7. Direito à Limitação do Tratamento 75
2.2.8. Direito de Portabilidade de Dados 78
2.2.9. Direito a Bloqueio ou Restrição do Processamento 79
2.2.10. Direito à Intervenção Humana na Tomada de Decisão e Criação de Perfil Automatizadas 80
2.2.11. Limitações 82
2.3. Transferência Internacional de Dados ou Processamento Transfronteiriço 82
2.3.1. Decisão de Adequação 83
2.3.2. Consentimento 85
2.3.3. Contrato 86
2.3.4. Regras Vinculativas Aplicáveis às Empresas 88
2.3.5. Certificados e Códigos de Conduta 90
3. Conclusões acerca das principais divergências e convergências entre a LGPD e a APPI 91
4. Aspectos convergentes e divergentes entre a LGPD e a PIPA 92
4.1. Autoridade de proteção de dados 93

4.1.1. Autônoma/Independente 93
4.1.2. Apresentação Unitária 94
4.2. Titulares de Dados 94
4.2.1. Definição 95
4.2.2. Direito de ser informado 95
4.2.3. Direito de Acesso 96
4.2.4. Direito à Retificação 97
4.2.5. Direito ao Esquecimento ou Direito ao Apagamento 98
4.2.6. Direito à Revogação 98
4.2.7. Direito à Limitação do Tratamento 99
4.2.8. Direito de Portabilidade de Dados 100
4.2.9. Direito a Bloqueio ou Restrição do Processamento 101
4.2.10. Direito à Intervenção Humana na Tomada de Decisão e Criação de Perfil Automatizadas 102
4.2.11. Limitações 103
4.3. Transferência Internacional de Dados ou Processamento Transfronteiriço 104
4.3.1. Decisão de Adequação 105
4.3.2. Consentimento 106
4.3.3. Contrato 106
4.3.4. Regras Vinculativas Aplicáveis às Empresas 107
4.3.5. Certificados e Códigos de Conduta 108
5. Conclusões acerca das principais divergências e convergências entre a LGPD e a PIPA 109

CONCLUSÃO 112

REFERÊNCIAS BIBLIOGRÁFICAS 114

Anexo 1 - Tabela comparativa entre APPI (Japão) e PIPA (Coreia do Sul), pela ótica dos 51 subtipos de instituições jurídicas do Modelo TLICS. 118

Resumo

A presente pesquisa tem o objetivo de promover a comparação entre a Lei nº 13.709/18, ou Lei Geral de Proteção de Dados Pessoais (LGPD), e outros dois diplomas normativos, quais sejam, a Lei sobre a Proteção de Informações Pessoais do Japão (acrônimo em inglês APPI) e a Lei de Proteção de Informações Pessoais da Coreia do Sul (acrônimo em inglês PIPA). Para isso, será utilizado o Modelo TLICS (*Telecommunications Law Indicators for Comparative Studies)*, o qual identifica as garantias institucionais promovidas pela LGPD para a realização do direito à privacidade, permitindo que essas sejam utilizadas como parâmetro para a identificação das mesmas variáveis nas leis japonesa e coreana, de forma que seja possível a investigação do grau de compatibilidade da proteção de dados pessoais promovida por esses países.

Em sua estrutura, este trabalho apresenta, primeiramente, uma introdução, a qual exibe os principais pontos a serem explorados pela pesquisa, dentre eles, qual sua relevância, qual a justificativa para o seu recorte geográfico orientado para o Japão e para a Coreia do Sul, qual a metodologia de análise, adiantando-se que é o modelo TLICS e, por fim, quais resultados são esperados desta investigação.

O primeiro capítulo, por sua vez, se debruça sobre a análise histórica da importância da proteção de dados pessoais e examina, do ponto de vista jurídico, o desenvolvimento deste direito até o estágio atual. Além disso, o tópico se dedicará à compreensão do Modelo TLICS e de seus indicadores de proteção de dados pessoais.

O segundo capítulo parte para a análise empírica da legislação do Brasil, do Japão e da Coreia do Sul, esmiuçando quais as garantias de proteção de dados oferecidas por cada uma, pela ótica do Modelo TLICS.

As informações a serem extraídas desse capítulo serão melhor exploradas no terceiro, o qual comparará o arcabouço jurídico do Brasil e do Japão e do Brasil e da Coreia do Sul, a fim de se evidenciar as semelhanças, as diferencias e as ausências, em termos de proteção de dados pessoais, apresentadas por estas leis.

O trabalho é finalizado com a conclusão, a qual estabelece, após os juízos de comensurabilidade elaborados no capítulo anterior, que há compatibilidade na proteção de dados pessoais entre Brasil e Japão e entre Brasil e Coreia do Sul. Dessa maneira, é possível que a transferência internacional de dados pessoais para estes dois países seja feita em conformidade com os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD).

Palavras-chaves: Proteção de Dados Pessoais; Brasil; Japão; Coreia do Sul; Modelo TLICS.

Abstract

This final project aims to compare the Law no. 13,709/18, or General Law for the Protection of Personal Data (Portuguese acronym LGPD), with two other legal statutes, namely, the Japanese Act on Protection of Personal Information (APPI) and the South Korean Personal Information Protection Act (PIPA). For this purpose, it uses the TLICS Model (Telecommunications Law Indicators for Comparative Studies), which identifies the institutional guarantees promoted by the LGPD to accomplish the right to privacy, which are applied to compare the Brazilian legal features with the Japanese and in the Korean laws on personal data protection, in order to investigate the degree of compatibility in terms of personal data protection promoted by these countries.

This work presents an introduction that shows the main points to be explored by this final project: what is the relevance of it, why to choose Japan and South Korea, what is the methodological approach, which is the Model TLICS as just mentioned, and what results are expected from this investigation.

The first chapter provides a historical analysis of the importance of personal data protection and examines the development of this right until the present stage, from a legal point of view. In addition, the chapter will seek to understand the TLICS Model and its personal data protection indicators.

The second chapter analyzes the legislation of Brazil, Japan and South Korea, and lists the guarantees of personal data protection offered by each one, through the lenses of the TLICS Model.

The third chapter will explore the discoveries from the chapter above when comparing the Brazilian legal framework with the Japanese one, and the Brazilian's with the South Korean's, to highlight the similarities, differences and absences, in terms of personal data protection presented by these laws.

In its final chapter, this work concludes that there is compatibility in terms of protection of personal data between Brazil and Japan and between Brazil and South Korea. Thus, it is possible that the international transfer of personal data to these two countries is done in accordance with the principles of the General Personal Data Protection Act (Portuguese acronym LGPD).

Keywords: Personal Data Protection; Brazil; Japan; South Korea; TLICS Model.

Lista de Tabelas

Tabela 1 – Formas institucionais e instituições legais de proteção de dados pessoais, conforme o Modelo TLICS 36

Tabela 2 – Formas institucionais, instituições legais e seus subtipos selecionados para análise da comensurabilidade entre as leis de proteção de dados do Brasil, do Japão e da Coreia do Sul 39

Lista de Acrônimos

ANPD	*Autoridade Nacional de Proteção de Dados*
APPI	*Act on the Protection of Personal Information*
BCRs	*Binding Corporate Rules*
CNPD	*Conselho Nacional de Proteção de Dados Pessoais e da Privacidade*
IBGE	*Instituto Brasileiro de Geografia e Estatística*
LGPD	*Lei Geral de Proteção de Dados Pessoais*
OMS	*Organização Mundial da Saúde*
P&D	*Pesquisa e Desenvolvimento*
PIHBO	*Personal Information Handling Business Operator*
PIPA	*Personal Information Protection Act*
RGPD	*Regulamento Geral sobre a Proteção de Dados*
STF	*Supremo Tribunal Federal*
TIC	*Tecnologias da Informação e Comunicação*
TLICS	*Telecommunications Law Indicators for Comparative Studies*

INTRODUÇÃO

O estudo consiste na análise das variáveis institucionais de proteção de dados pessoais presentes em arcabouços jurídicos de diferentes países, mais precisamente do Brasil, do Japão e da Coreia do Sul, a partir do Modelo TLICS.

Primeiramente, importa contextualizar o instituto da proteção de dados pessoais na história. Em relação ao desenvolvimento da sociedade, pode-se falar, ainda que de forma muito simplificada, primeiro do surgimento de uma sociedade agrícola, voltada para a terra, depois de uma sociedade industrial, ligada à produção, em seguida, de uma sociedade pós-industrial, orientada para a oferta de serviços, e, atualmente, de uma sociedade da informação, voltada para o fluxo informacional (BIONI, 2020, p. 3).

Os antecedentes que deram origem a esta sociedade da informação remontam à Segunda Guerra Mundial e anos seguintes, quando ocorreu o surgimento das principais descobertas em eletrônica, a exemplo do computador programável e do transistor (CASTELLS, 2005, p. 76). Porém, foi na década de 1970, com a vasta disseminação das tecnologias da informação e da comunicação (TIC), que eclodiu esse novo paradigma na história (CASTELLS, 2005, p. 76), essa nova estrutura social, também chamada de informacionalismo, a qual visa o desenvolvimento tecnológico, a acumulação de conhecimento e o atingimento de maiores níveis de complexidade de processamento de informação (CASTELLS, 2005, p. 51; 54). Tanto é assim que, hoje, se fala em uma nova economia, a qual é: informacional, porquanto é a capacidade dos agentes econômicos de gerar e processar eficientemente as informações que vai definir sua produtividade e competitividade; global, tendo em vista as atividades produtivas, de consumo e de circulação estarem organizadas em uma escala global; e, em rede, pelo fato de a produtividade e a concorrência serem realizadas em uma rede global de interação entre redes empresariais (CASTELLS, 2005, p. 119).

À medida em que as TIC se amplificavam, as discussões acerca do direito à privacidade e, consequentemente, à proteção de dados também se desenvolviam. Hoje o direito à privacidade é visto como uma garantia do controle das próprias informações pelo indivíduo e um requisito para a realização de um Estado Democrático de Direito (SCHERTEL, 2014, p. 29). Mostra disso é o

recente caso de gerenciamento de dados obtidos no meio informacional envolvendo a empresa *Cambridge Analytica* e o *Facebook*, para fins de direcionamento de propaganda política durante as eleições americanas de 2016.

Assim, acompanhando a tendência de outros países no mundo, é promulgada no Brasil, em 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (Lei nº13.709/18), inspirada no Regulamento Geral Europeu sobre a Proteção de Dados (RGPD), aprovado em 2016 (MENDES e DONEDA, 2018, p. 470). A Lei 13.709/18 se aplica às operações de tratamento de dados pessoais que ocorram no Brasil, ou que tenham por objetivo a oferta, o fornecimento de bens ou o tratamento de dados de pessoas localizadas no país, ou ainda, se aplica às operações que visam o tratamento de dados que tenham sido coletados aqui.

No entanto, em função da existência de uma sociedade da informação e do desenvolvimento das TIC, todos os dias os mais variados países do mundo estão envolvidos em um intenso fluxo de transferência de dados pessoais. Atenta a essa realidade, a LGPD disciplinou no seu art. 33, inciso I, que a transferência internacional de dados pessoais somente é permitida para países ou organismos internacionais que proporcionem grau de proteção adequado ao previsto na lei. Assim, é essencial a análise das legislações de outros territórios voltadas para proteção de dados pessoais, a fim de identificar esta adequação.

Dessa forma, neste estudo estarão sob análise a Lei sobre a Proteção de Informações Pessoais do Japão (acrônimo em inglês APPI), adotada pelo país em 2003 e atualizada em 2020, e a Lei de Proteção de Informações Pessoais da Coreia do Sul (acrônimo em inglês PIPA), adotada em 2011 e com última atualização também em 2020.

A justificativa para o foco da pesquisa estar sobre esses dois países se dá pelo fato de serem grandes polos asiáticos de desenvolvimento tecnológico e, portanto, importantes atores quando se considera fluxo de dados, inclusive os pessoais. Para fins de comparação com o cenário brasileiro, a *Global Innovation 1000 Study*[1]*,* que realiza anualmente um estudo acerca das 1000 maiores empresas investidoras em pesquisa e desenvolvimento (P&D) no mundo, incluiu

[1]Disponível em: https://www.strategyand.pwc.com/gx/en/insights/innovation1000.html#VisualTabs1. Acesso em: 27/03/2020.

no seu *ranking* de 2018, 7 empresas japonesas, 5 sul-coreanas e apenas uma brasileira, considerando-se aqui as que atuam nas indústrias de "*Software* e Serviços" e de "Serviços de Telecomunicação". Para além disso, esse mesmo estudo indica que as referidas empresas japonesas juntas investiram 6,2 bilhões de dólares em P&D e, em média, cada uma disponibilizou 9,36% das suas receitas para este fim. As empresas coreanas, por sua vez, destinaram 2,1 bilhões de dólares para P&D e, em média, cada uma direcionou 8,02% das suas receitas para isso. A única empresa brasileira no *ranking* reservou 16,4% das suas receitas para P&D, mas, em valores brutos, isso representou 0,1 bilhão de dólar.

Para inferir qual o grau de compatibilidade referente à proteção de dados que esses países compartilham, será aplicado o Modelo TLICS, o qual viabiliza a correlação de variáveis legais na medida em que dispõe as garantias institucionais em uma estrutura teórica capaz de elucidar conceitos jurídicos importantes relacionados à proteção de dados pessoais (ARANHA, MENDES, *et al.*, 2019, p. 142). O uso do Modelo torna viável a aferição da presença ou da ausência das variáveis jurídicas identificadas na LGPD, nos diplomas legais do Japão e da Coreia do Sul.

A partir dessa aplicação, será possível fazer uma análise com o intuito de responder ao questionamento a que se presta este trabalho: qual o grau de equivalência da proteção de dados existente na APPI e na PIPA em comparação com a LGPD. Em outras palavras, seria permitida a transferência internacional de dados pessoais entre Brasil e Japão e entre Brasil e Coreia do Sul, em decorrência de um nível de proteção de dados semelhante?

A expectativa é que a resposta a esta pergunta seja positiva, esperando-se encontrar um elevado grau de compatibilidade da LGPD em relação à APPI e à PIPA, pelos indícios elencados a seguir.

A Lei Geral de Proteção de Dados Pessoais do Brasil, conforme verificado pela aplicação do Modelo TLICS, atende às determinações da União Europeia quanto aos padrões de proteção de dados (ARANHA, MENDES, *et al.*, 2019, p. 144-146). Por sua vez, em janeiro de 2017, a Comissão Europeia lançou comunicado ao Parlamento Europeu indicando que o Japão e a Coreia do Sul tinham modernizado recentemente a sua legislação, visando instituir regimes abrangentes em matéria de proteção de dados. Afirmou também que daria

prioridade sobre eventuais decisões de adequação com o principais parceiros comerciais do Leste e do Sudeste Asiático, começando justamente pelo Japão e pela Coreia do Sul (EUROPEIA, 2017, p. 9). Em seguida, a Lei sobre a Proteção de Informações Pessoais do Japão (APPI) foi considerada comparável ao RGPD, em termos de proteção de dados pessoais, pela Comissão Europeia, na Decisão de Execução (EU) 2019/419, de 23 de janeiro de 2019 (EUROPEIA, 2019a, p. 2). Em relação à Coreia do Sul, em março de 2021 foi anunciado que as deliberações entre o país e a Comissão Europeia confirmaram o alto grau de convergência entre o RGPD e a PIPA, de forma de uma decisão de adequação deve ser firmada assim que possível (EUROPEIA, 2021).

Portanto, ao que tudo indica, há comensurabilidade entre esses diplomas, pelo fato de todos terem nível de proteção de dados comparável ao oferecido pelo modelo europeu. Ao longo dos próximos capítulos esta pesquisa se prestará a testar esta hipótese, por meio da aplicação do Modelo TLICS aos arcabouços jurídicos do Japão e da Coreia do Sul, em comparação à legislação brasileira.

CAPÍTULO 1: Desenvolvimento normativo do direito à proteção de dados pessoais e os indicadores de proteção presentes no Modelo TLICS

1.1. O desenvolvimento do direito à proteção de dados pessoais

A matéria de proteção de dados pessoais sofreu diversas alterações nos últimos 40 anos, em função das diversas transformações econômicas, sociais e tecnológicas que ocorreram ao longo dessas décadas (SCHERTEL, 2014, p. 37). Em um estágio mais avançado de desenvolvimento do tema, o direito à proteção de dados pessoais se apresenta como matéria autônoma em diversos ordenamentos jurídicos (DONEDA, 2011, p. 96). Ou seja, cada vez mais se compreende o direito à proteção de dados pessoais como uma espécie do gênero direitos fundamentais (MAÑAS, 2005, p. 18), para além da sua relação com o direito à privacidade somente.

Essa progressão histórica pode ser verificada a partir da escala das quatro gerações de leis voltadas para a tutela de dados pessoais, criada por Viktor Mayer-Scönberger (DONEDA, 2011, p. 96), a qual será exposta nos tópicos subsequentes deste subtítulo.

1.1.1. A primeira geração de leis de proteção de dados pessoais

Conforme já abordado na introdução deste trabalho, a revolução tecnológica iniciada na Segunda Guerra Mundial transformou a capacidade de processamento de informações, tanto quantitativamente, quanto qualitativamente (BIONI, 2020, p. 109). A partir disso, iniciou-se um movimento de criação de bancos de dados unificados de grande porte, os quais cumulavam as tarefas de coleta e gestão das informações de seus cidadãos, com o objetivo de serem utilizadas para o planejamento das ações governamentais (BIONI, 2020, p. 109), em um contexto de concretização de um Estado Social (SCHERTEL, 2014, p. 38).

Pode-se se citar, como exemplos do esforço realizado por máquinas públicas do período para a coleta de dados de seus cidadãos, o que ocorreu na Suécia, na Alemanha e nos Estados Unidos (SCHERTEL, 2014, p. 38). No caso da Suécia, o parlamento propôs, em 1960, a fusão de todas as informações fiscais, registros civis e dados do censo e, já na Alemanha, o governo criou um comitê com o objetivo de vincular os bancos de dados municipais, estaduais e

federal (SCHERTEL, 2014, p. 38). No mesmo sentido, nos Estados Unidos, em 1965, o "*Bureau of Budget*", órgão responsável pela gerência orçamentária, propôs a criação do "*National Data Center"* (GARFINKEL, 2000, p. 13)*. A* intenção era reduzir os gastos governamentais, sob a justificativa de que os demais órgãos do governo não precisariam investir em tecnologia, tendo em vista que existiria um centro de dados nacional único (SCHERTEL, 2014, p. 39). Em determinado momento, se defendeu que diversos tipos de dados deveriam compor o banco, a exemplo de data de nascimento, cidadania, registro escolar, serviço militar, registro de impostos, benefícios da previdência social, registro do espólio e, até mesmo, registros criminais (SCHERTEL, 2014, p. 39). A extensão da quantidade de informações requeridas e, consequentemente, do poder que o Estado teria, seria tão grande, que diversas discussões se suscitaram na sociedade americana acerca da inadequação da criação de tal banco de dados (SCHERTEL, 2014, p. 39). Como consequência, não se permitiu que o projeto fosse posto em prática (SCHERTEL, 2014, p. 39).

Fica visível, assim, o receio dos cidadãos de que as suas liberdades fossem suprimidas em função de uma vigilância ostensiva, do que decorre a necessidade de regular a própria tecnologia, conformando-a aos valores democráticos (BIONI, 2020, p. 110). Surge, dessa forma, a primeira geração de leis de proteção de dados pessoais, na década de 70 (BIONI, 2020, p. 110).

As leis de primeira geração buscavam exercer o controle por meio da exigência de autorização para o funcionamento dos bancos de dados e, também, por meio da regulação do uso, pelas estruturas administrativas do Estado, das informações dos cidadãos, salientando-se que, à época, esses dados eram dirigidos quase que unicamente àqueles órgãos (DONEDA, 2011, p. 96). Conclui-se, então, que o foco destas normas era o processamento de dados e seus agentes responsáveis, deixando à parte os cidadãos (DONEDA, 2011, p. 96). Como consequência destas normas se voltarem, essencialmente, ao rígido controle dos procedimentos, a garantia ao direito à privacidade não era uma prioridade, o que fica ainda mais evidente quando se leva em consideração os termos técnicos que as constituíam (SCHERTEL, 2014, p. 39).

De forma paradoxal, os Estados não conseguiram proceder à criação desses bancos de dados massivos e centralizados não tanto pelas críticas advindas da sociedade, mas, sim, pelo avanço tecnológico que viabilizou o

processamento de informações por mais sujeitos, descentralizando esse procedimento (SCHERTEL, 2014).

Dessa forma, na esfera pública, pequenas e pulverizadas unidades do governo passaram a manejar dados, assim como sujeitos externos à estrutura governamental, pertencentes à iniciativa privada (SCHERTEL, 2014). Como consequência, a quantidade de bancos de dados a serem regulados e autorizados cresceu, se tornando inevitável o desenvolvimento de uma segunda geração de leis relacionadas à proteção de dados pessoais (BIONI, 2020, p. 110). Procurou-se, também, corrigir o fato de as leis de primeira geração priorizarem o procedimento ao invés dos direitos dos cidadãos (SCHERTEL, 2014, p. 40).

Pode-se exemplificar esta geração de normas pelas leis do Estado alemão de Hesse, de 1970; a Lei de Dados da Suécia, de 1973; o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz, de 1974; e a Lei Federal de Proteção de Dados da Alemanha, de 1977 (SCHERTEL, 2014, p. 38). Importa ressaltar que, embora algumas dessas leis tenham surgido no final da década de 70, quando já imperava o desenvolvimento das normas de segunda geração, todas elas são classificadas como de primeira em função de sua estrutura e linguagem coerentes com a fase (SCHERTEL, 2014, p. 38).

1.1.2. Segunda geração de leis de proteção de dados pessoais

Com a difusão dos bancos de dados informatizados, o Estado se viu incapaz de controlar a criação e o funcionamento de todas essas bases (BIONI, 2020, p. 110). A desconfiança em relação à criação de um banco de dados único e centralizado, deu lugar ao temor pela multiplicação dos bancos de dados ao redor do globo, conectados em rede e administrados tanto por organizações públicas quanto privadas (SCHERTEL, 2014, p. 40). Surge, assim, da necessidade de adoção de outra estratégia de regulação (BIONI, 2020, p. 110), no final da década de 70, a segunda geração de leis de proteção de dados pessoais (DONEDA, 2011, p. 97).

Segundo esta nova abordagem, a reponsabilidade pela proteção de dados pessoais deveria ser transferida ao cidadão, tendo em vista a incapacidade da máquina administrativa de fazê-lo, quando tantos bancos de dados passam a existir (BIONI, 2020, p. 110). O instrumento a ser usado pelo

indivíduo para proteger as suas informações é o consentimento, devendo, portanto, fazer as escolhas relacionadas ao processamento de seus dados (BIONI, 2020, p. 110).

Assim, diferentemente das normas de primeira geração, focadas nos procedimentos para proteção de dados, as leis de segunda geração adotaram, como tática para a tutela das informações pessoais, a garantia do direito à privacidade e das liberdades negativas e individuais das pessoas (SCHERTEL, 2014, p. 40). Esses deveriam ser direitos suficientemente fortes, o quais poderiam, caso necessário, ter até mesmo previsão constitucional (SCHERTEL, 2014, p. 40).

Como exemplo de normas de segunda geração estão as leis da Áustria, da França, da Dinamarca e da Noruega, além das previsões encontradas nas constituições da própria Áustria, da Espanha e de Portugal (SCHERTEL, 2014, p. 40).

As leis de segunda geração, no entanto, foram alvo de algumas críticas. Em primeiro lugar, havia uma incerteza quanto ao grau de efetividade do consentimento do cidadão como instrumento para a proteção de dados pessoais e, em segundo lugar, se questionava quão autônomo era o indivíduo para fornecer ou não suas informações, tendo em vista que, ao não fazê-lo, poderia ser excluído de relações sociais de diversos tipos (SCHERTEL, 2014, p. 41). Exemplo dessas relações são a abertura de contas bancárias, o processo para habilitação da carteira de motorista e a doação sangue, as quais todas exigem a disposição de dados pessoais para se efetivarem (PEZZENELLA e WENCZENOVICZ, 2015, p. 104).

Essa realidade é consequência do avanço tecnológico, por meio do qual mais entes públicos e privados passaram a se valer de dados pessoais para realizar suas atividades, de forma que o fornecimento dessas informações pelo cidadão se tornou imprescindível à sua efetiva participação na sociedade (DONEDA, 2011, p. 97). Do ponto de vista da esfera pública, os dados pessoais são essenciais para o funcionamento da máquina burocrática, que é quem põe em prática os projetos do Estado Social (SCHERTEL, 2014, p. 41). Já do ponto de vista da esfera privada, a mesma dificuldade é identificada, considerando-se que, em uma sociedade regida pelo mercado de consumo, os fornecedores somente estariam dispostos a oferecer determinados serviços mediante o

provimento de certos dados pessoais pelo consumidor (SCHERTEL, 2014, p. 41).

Surge, dessa forma, a necessidade de uma nova abordagem a ser conferida pelas leis de proteção de dados pessoais.

1.1.3. Terceira geração de leis de proteção de dados pessoais

Na década de 80 desponta a terceira geração de leis de proteção de dados pessoais (DONEDA, 2011, p. 97). Por causa das novas tecnologias de rede e telecomunicações que surgiram, os bancos de dados não são mais estabelecidos fisicamente, mas, sim, em redes, sem uma central identificável de processamento, o que possibilita a sua rápida transferência (SCHERTEL, 2014, p. 42).

O paradigma deste período foi a decisão da Corte Constitucional alemã em relação à Lei do Censo de 1983 (BIONI, 2020, p. 111). Segundo esta lei, os cidadãos alemães deveriam informar uma série de dados pessoais para a aferição da distribuição espacial e geográfica da população (BIONI, 2020, p. 97). No entanto, por meio de redação vaga, a lei previa que os dados coletados poderiam ser cruzados com outros registros públicos para fins de realização de “atividades administrativas” (BIONI, 2020, p. 97).

Ao analisar o caso, o Tribunal Constitucional alemão entendeu que os indivíduos tinham direito à autodeterminação informativa, mediante uma reinterpretação da Lei Federal de Proteção de Dados Pessoais da Alemanha à luz da Lei Fundamental de Bonn (SCHERTEL, 2014, p. 41) e exigiu que as informações pessoais dos cidadãos servissem apenas às estatísticas do recenseamento (BIONI, 2020, p. 97).

Assim, a terceira geração de leis de proteção de dados pessoais permanece focada nas escolhas do cidadão para a tutela das suas informações (DONEDA, 2011, p. 97). No entanto, a ideia de autodeterminação informativa expande, em muito, a participação do indivíduo nesse processo, o qual começa a estar continuamente inserido no processamento de seus dados pessoais, desde a coleta até a transmissão, passando pelo armazenamento (SCHERTEL, 2014, p. 41-42).

Além disso, com a decisão do Tribunal Constitucional alemão, fica estabelecido que a autodeterminação dos dados pelo indivíduo é essencial para

o exercício do seu direito de desenvolver a sua personalidade, o qual seria, inclusive, um direito autônomo (BIONI, 2020, p. 99-100). Não se pode perder de vista que os dados pessoais são elementos constitutivos da personalidade, pois têm origem no indivíduo, revelando sua identidade e seus comportamentos (ROCHFELD, 2018, p. 73).

Em suma, o julgado é paradigmático porque dele surge o termo autodeterminação informacional ou autodeterminação informativa; a ideia de que o direito à proteção de dados pessoais é autônomo, ou seja, separado e, portanto, diferente do direito à privacidade; e, por fim, o entendimento de que o direito à proteção de dados pessoais pertence ao rol dos direitos da personalidade (BIONI, 2020, p. 98).

São exemplos de leis de terceira geração as dos Estados alemães após a decisão do Tribunal Constitucional do país, a emenda à Lei Federal de Proteção de Dados Pessoais da Alemanha, de 1990, a emenda à lei da Áustria, de 1986, a alteração feita na lei da Noruega e a previsão de proteção de dados pessoais presente na constituição holandesa (SCHERTEL, 2014, p. 42).

O caso levado à Corte Constitucional alemã permanece atual na medida em que é possível traçar paralelos entre a Lei do Censo de 1983 e a Medida Provisória nº 954 de 17 de abril de 2020, a qual objetiva promover a produção estatística oficial no Brasil, durante a crise sanitária desencadeada pela pandemia de coronavírus (vírus esse oficialmente nomeado pela Organização Mundial da Saúde (OMS) como SARS-COV-2[2], causador da doença COVID-19[3]).

Conforme o art. 2º desta medida provisória, empresas de telecomunicação deveriam disponibilizar ao Instituto Brasileiro de Geografia e Estatística (IBGE[4]), em meio eletrônico, a relação de nomes, números de

---

[2] Disponível em: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it. Acesso em: 06/05/2020.

[3] Segundo a Organização Mundial da Saúde (OMS), a COVID-19 é a doença infecciosa causada por um coronavírus desconhecido antes do surto que ocorreu em Wuhan, China, em dezembro de 2019. O órgão declarou, em 11 de março de 2020, que a presença do vírus no mundo passava a ser considerada uma pandemia. Disponível em: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/q-a-coronaviruses e https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020. Acesso em: 06/05/2020.

[4] O IBGE, entidade da administração pública federal, se constitui, segundo informações extraídas de seu sítio eletrônico, no principal provedor de dados e informações do Brasil e, dentre as suas

telefones e endereços de seus consumidores, sejam eles pessoas físicas ou jurídicas. Ainda conforme o § 1º desse artigo, o objetivo da coleta desses dados é a realização de entrevistas em caráter não presencial, o que seria coerente com as medidas de isolamento social requeridas da população e necessárias ao combate à pandemia, segundo orientação da OMS[5].

No entanto, ainda que o art. 3º, II, reforce que essas informações serão utilizadas exclusivamente para a elaboração de estatísticas pelo órgão, importa ressaltar, em primeiro lugar, o excesso de dados oficiais requisitados, como endereço, tendo em vista que as entrevistas seriam realizadas remotamente, e, em segundo lugar, a falta de maiores detalhes acerca de quais pesquisas serão executadas a partir desse material (MACIEL, 2020), ficando seu escopo genericamente definido pelo termo "*produção estatística oficial*" (art. 2º, §1º). Ainda que no caso brasileiro não exista previsão para o cruzamento, com outros registros públicos, das informações cedidas ao IBGE, a finalidade do uso desses dados foi muito vagamente descrita, semelhantemente ao que se encontrou na Lei do Censo de 1983 da Alemanha.

O caso revela que, ainda hoje, existem legislações sobre proteção de dados pessoais que muito aproveitariam se observassem as orientações advindas do que o Tribunal Constitucional alemão julgou na década de 80.

Nesse sentido, em decisão de importância comparável à alemã, o Supremo Tribunal Federal (STF) suspendeu a aplicação da MP nº 954/2020 (MENDES, 2020). O julgamento do plenário, que ocorreu sob a relatoria da Min. Rosa Weber nos dias 06 e 07 de maio de 2020, acatou a medida cautelar nas Ações Diretas de Inconstitucionalidade nº 6.387, nº 6.388, nº 6.389, nº 6.393 e nº 6.390 (MENDES, 2020). Segundo o voto da Min. Relatora, a MP 954/2018 enseja riscos decorrentes de sua generalidade, ausência de medidas de segurança e coleta excessiva de dados (MENDES, 2020).

Assim, a decisão da Corte elevou o status da proteção de dados pessoais no Brasil, ao reconhecê-la expressamente como um direito fundamental autônomo, garantido pela Constituição Federal (MENDES, 2020). Este

---

atividades, está a de produção e análise de informações estatísticas. Disponível em: https://www.ibge.gov.br/institucional/o-ibge.html. Acesso em: 06/05/2020.

[5] Disponível em: https://g1.globo.com/jornal-nacional/noticia/2020/03/30/oms-reforca-que-medidas-de-isolamento-social-sao-a-melhor-alternativa-contra-o-coronavirus.ghtml. Acesso em: 07/05/2020.

movimento indicou uma evolução do entendimento do STF presente em julgados como o RE 418.416-8/SC Relator Min. Sepúlveda Pertence, 10/05/2006 e o HC 91.867/PA, Relator Min. Gilmar Mendes, 24/04/2012, assemelhando a tutela de proteção de dados à autodeterminação informativa estabelecida na Alemanha. (MENDES, 2020). Os Min. Rosa Weber, Gilmar Mendes e Luiz Fux, inclusive, fazem menção ao acórdão do Tribunal Constitucional alemão e à Carta de Direitos Fundamentais da União Europeia (MENDES, 2020).

Quanto às normas de terceira geração de modo geral, o questionamento que se fez a elas foi o mesmo feito às leis de segunda geração: quão eficaz poderia ser a tutela de dados pessoais, realizada por meio do consentimento, tendo em vista ser esse um instrumento demasiadamente centrado no poder de escolha dos cidadãos, em um contexto em que a participação do indivíduo nas mais variadas relações sociais, o obrigava a dispor de suas informações (BIONI, 2020, p. 112). Em outras palavras, quão factual é o poder do indivíduo de autodeterminar seus dados? Além disso, uma outra crítica que se impunha é a de que o cidadão não poderia pedir reparação quando da violação do seu direito à privacidade, pelo fato do seu consentimento ter autorizado o processamento e o tratamento de seus dados pessoais (SCHERTEL, 2014, p. 42-43).

Concluiu-se, assim, que todo aquele arquétipo de efetiva participação dos cidadãos no controle de suas informações pessoais, angariada pela autodeterminação informativa, não poderia se concretizar realmente (SCHERTEL, 2014, p. 42). A quarta geração de leis de proteção de dados pessoais surge, dessa forma, como uma tentativa de corrigir os equívocos gerados pela confiança excessiva no consentimento como resposta para tutela de dados pessoais.

1.1.4. Quarta geração de leis de proteção de dados pessoais

A quarta geração de leis de proteção de dados pessoais surge na década de 90. No entanto, antes de se prosseguir à caracterização das normas do período, importa contextualizar os avanços tecnológicos nos anos 1990 e 2000, sobretudo no que diz respeito à Internet.

Na década de 90, a rede mundial de computadores era definida como *web 1.0* e poderia ser comparada a uma ferramenta de leitura, tendo em vista funcionar, basicamente, como meio de comunicação por *e-mails* e fonte de

informações (LIMA, 2015, p. 120). A mudança dessa estrutura ocorre na década seguinte, com o aumento dos recursos da rede e a possibilidade de produção de conteúdo de forma colaborativa, o qual, através da *web 2.0*, poderia ser vastamente divulgado, permitindo que outros usuários continuassem interagindo com o seu teor (LIMA, 2015, p. 120).

Como consequência desses avanços, quantidades gigantescas de informação passam a ser introduzidas na rede mundial de computadores e recursos começam a ser desenvolvidos por aqueles que manejam esses dados, a exemplo das ferramentas de busca (*search engines*), do *big data*[6] e do *cloud computing* (LIMA, 2015, p. 120-121). Logo se percebeu que dados poderiam ser monetizados através de procedimentos lucrativos, como o *marketing* comportamental, o uso de *cookies* e a elaboração de *big data* (LIMA, 2015, p. 121). Como essas ferramentas são alimentadas por dados, várias atividades, como a manutenção de perfis em redes sociais, passaram a ser oferecidas gratuitamente, a fim de que ainda mais informações fossem inseridas na rede (LIMA, 2015, p. 121). Pode-se inferir, assim, que, na sociedade informacional, o processamento de dados pessoais tem cada vez mais ingerência na vida das pessoas, tendo em vista estarem elas inseridas em uma economia que se orienta e se alimenta das informações identificadoras dos cidadãos (BIONI, 2020, p. 57).

Esses dados constituem a identidade do indivíduo (BIONI, 2020, p. 57), e, como consequência, estão cada vez mais relacionados aos direitos de personalidade de seus titulares (BIONI, 2020, p. 57), de forma que a coleta, a administração e o armazenamento dessas informações passaram a demandar nova legislação sobre proteção de dados pessoais (LIMA, 2015, p. 121). Assim, neste novo contexto, fica estabelecido que as escolhas dos indivíduos não são suficientes para a salvaguarda de seus dados, sendo necessário se elevar o padrão coletivo de proteção (DONEDA, 2011, p. 98).

Entre as técnicas utilizadas para alcançar este fim, pode-se citar, em primeiro lugar, o reconhecimento do desiquilíbrio da relação entre os titulares de dados pessoais e as instituições que realizam a coleta e processamento dessas informações, admitindo-se a necessidade de elevação da posição dos cidadãos,

---

[6] "[...] o Big Data representa o êxtase desse processo [o progresso quantitativo e qualitativo da gestão da informação]. Essa tecnologia permite que um volume descomunal de dados seja estruturado e analisado para uma gama indeterminada de finalidades" (BIONI, 2020, p. 34).

tendo em vista que o simples reconhecimento do direito à autodeterminação informativa não seria suficiente para aplacar esta assimetria (DONEDA, 2011, p. 98). Assim, as normas passaram a objetivar o fortalecimento da posição do indivíduo pelo aumento da efetividade do seu controle sobre seus dados pessoais (SCHERTEL, 2014, p. 43). Como exemplo de recurso para concretização desta estratégia, pode-se referir à previsão de "*no fault compensation*"[7], caso o indivíduo veja o seu direito à proteção de dados pessoais transgredido (SCHERTEL, 2014, p. 43). Isso se deu com uma emenda à Lei Federal de Proteção de Dados alemã, observando-se que, em menor escala, norma parecida já estava presente na legislação norueguesa (SCHERTEL, 2014, p. 43).

Em segundo lugar, com o fim de elevar o padrão geral de proteção de dados pessoais, buscou-se reduzir o papel individual de autodeterminação informativa, considerando-se que certos dados, a exemplo dos sensíveis, devem ser melhor protegidos (DONEDA, 2011, p. 98). Os dados sensíveis são aqueles que dizem respeito à origem racial e étnica, às convicções políticas, ideológicas e religiosas, às preferências sexuais, aos dados sobre a saúde, aos dados genéticos e aos biométricos (SARLET e CALDEIRA, 2019, p. 13).

Em terceiro lugar, houve o aumento e a difusão de autoridades independentes responsáveis pela aplicação das leis de proteção de dados pessoais, ainda mais necessárias em um contexto de descentralização do papel da autodeterminação informativa (DONEDA, 2011, p. 98).

Por fim, adotaram-se normas específicas para determinados setores de processamento de dados, a exemplo daqueles destinadas aos serviços de saúde e de crédito ao consumo (DONEDA, 2011, p. 98). Prova disso é a adesão de normas setoriais por diversos países a fim de complementar as normas gerais de proteção de dados pessoais, como ocorreu na maioria dos países europeus (SCHERTEL, 2014, p. 43-44).

Importa destacar que as leis de quarta geração não extinguiram o protagonismo do consentimento, mas relativizaram a sua centralidade (BIONI,

[7] "No-fault compensation refers to a compensation scheme based on the principle that injured persons are entitled to receive compensation for their injuries, without proving fault against the opposite party". Disponível em: https://definitions.uslegal.com/n/no-fault-compensation/. Acesso em 14/05/2020.

2020, p. 112), condicionando a sua eficácia à necessidade de apresentação de algumas qualidades (BIONI, 2020, p. 112), como o fato de dever ser livre, informado, inequívoco, explícito e específico (BIONI, 2020, p. 112).

O primeiro passo para o estabelecimento de uma quarta geração de leis no continente europeu ocorreu com a Diretiva Europeia sobre proteção de dados pessoais de 1995 (SCHERTEL, 2014, p. 44). Nela, pode-se observar a preocupação com a efetivação da participação do indivíduo no tratamento de seus dados pessoais e o condicionamento ao consenso expresso e informado do cidadão quanto ao processamento de seus dados sensíveis (SCHERTEL, 2014, p. 44). Esse recorte geracional perdura até os dias de hoje, abarcando, inclusive, a Lei Geral de Proteção de Dados Pessoais brasileira (LEME, 2019, p. 180).

Conclui-se, assim, que, em função, principalmente, das constantes mudanças tecnológicas, as leis relacionadas à proteção de dados pessoais sofreram mudanças importantes nas últimas quatro décadas (SCHERTEL, 2014, p. 44). No entanto, é possível identificar o desenvolvimento e fortalecimento da tutela à personalidade do cidadão, por meio, principalmente, da proteção à autodeterminação informativa e aos dados sensíveis (SCHERTEL, 2014, p. 44).

1.2. O Modelo TLICS como indicador de proteção de dados pessoais

O objetivo deste trabalho, conforme apresentado em sua introdução, é verificar se a LGPD (Lei 13.709/18) garante uma proteção de dados pessoais compatível com a tutela prevista nas legislações de mesma matéria presentes no Japão e na Coreia do Sul. A finalidade de se estabelecer qual o grau de convergência no que diz respeito à proteção de dados pessoais entre esses países é o cumprimento do art. 33, inciso I da LGPD, segundo o qual o fluxo internacional de dados pessoais somente deve se dar na presença dessa correspondência.

No entanto, antes de se prosseguir ao cotejamento das normas brasileira, japonesa e coreana, o qual se realizará nos próximos capítulos, faz-se necessário eleger alguma metodologia para este estudo comparativo. Nesse sentido, uma revisão bibliográfica para apontar alguns dos indicadores jurídicos

existentes em pesquisa comparada no âmbito das TIC foi realizada em Aranha e Oliveira (2016)[8].

A conclusão dos autores foi a de que a maior parte das metodologias se limita a discriminar arcabouços jurídicos em garantias institucionais, com o fim de identificar diferenças e semelhanças entre essas variáveis (ARANHA e OLIVEIRA, 2016, p. 3). Esse procedimento, no entanto, não é suficiente, visto que a mera semelhança de palavras não garante a existência de significados jurídicos compatíveis entre si, pois um mesmo vocábulo pode apresentar diferentes sentidos em países com tradições e estruturas legais diversas (ARANHA e OLIVEIRA, 2016, p. 4). Para resolver esse obstáculo, os autores sugerem uma nova abordagem hermenêutica aplicada à avaliação de compatibilidades em TIC: o chamado Modelo TLICS (*Telecommunications Law Indicators for Comparative Studies)* (ARANHA e OLIVEIRA, 2016, p. 19).

Esse modelo visa melhor especificar as variáveis institucionais que constituem os conceitos jurídicos presentes em diferentes estruturas legais, no intuito de aprofundar, aperfeiçoar e aumentar a utilidade das informações extraídas a partir da confrontação de suas semelhanças e diferenças (ARANHA e OLIVEIRA, 2016, p. 19-20). Ainda que a referida obra enfoque o uso do Modelo TLICS para o estudo do federalismo no campo das TIC, a metodologia será empregada nesta monografia para aferir a compatibilidade entre diferentes legislações quanto ao nível de proteção de dados pessoais, mais precisamente as do Brasil, do Japão e da Coreia do Sul.

O aprofundamento do que seja o Modelo TLICS se dará nos tópicos subsequentes.

1.2.1. O Modelo TLICS e suas teorias de apoio

O modelo TLICS emprega o uso da teoria hermenêutica prescritiva de Wilhelm Dilthey e de Emílio Betti e da teoria concretista da interpretação, promovida por Konrad Hesse (ARANHA e OLIVEIRA, 2016, p. 26). A metodologia também se apoia em outras duas teorias de suporte, mais precisamente, a teoria institucional do direito, elaborada por Santi Romano, e a teoria das garantias institucionais, fomentada por Carl Schmitt (ARANHA e

[8] Todas as citações desta obra se deram sob a forma de "livre tradução do autor".

OLIVEIRA, 2016, p. 26). Parte-se, assim, para a melhor compreensão da contribuição desses autores para a construção do Modelo TLICS.

1.2.1.1. A hermenêutica prescritiva de Emílio Betti no modelo TLICS

Emílio Betti (1890-1968) foi um jurista italiano, partidário da tradição da qual também fazem parte Schleiermacher e Dilthey, que buscou estabelecer uma teoria geral para a interpretação das objetivações da experiência humana (PALMER, 1969, p. 55). Nesse sentido, defendeu que a hermenêutica passasse a ser considerada também um problema epistemológico, ou seja, ligado ao processo do conhecimento (ROESLER, 1998, p. 9). Assim, parte de sua teoria da interpretação é voltada para a explicação e a fixação de regras para se atingir a compreensão (ROESLER, 1998, p. 9).

Segundo Betti, o processo interpretativo ocorre mediante duas condições: primeiramente, deve haver um outro espírito, diverso do que interpreta, e que se objetive em formas representativas (*sinnhaltige Formen*); em segundo lugar, é necessária a própria existência das formas representativas (SPAREMBERGER, 2003, p. 177). O entendimento entre interlocutores necessita, dessa forma, da objetividade do significado linguístico, assegurada quando as representações que esses mesmos interlocutores fazem são correspondentes (PESSÔA, 2002, p. 86).

Para o autor, o processo interpretativo é infinito, pois, sendo as formas representativas, incluindo aquelas determinadas como instituições jurídicas, a objetivação da criatividade de um outro espírito, devem ser analisadas de forma não arbitrária, ou seja, em conformidade com uma metodologia (ARANHA e OLIVEIRA, 2016, p. 22).

Nesse sentido, ainda mais especificamente quanto às declarações legais, a interpretação de um conceito jurídico requer uma metodologia própria de resgate da mensagem original (ARANHA e OLIVEIRA, 2016, p. 22). O que o autor percebe é que esses conceitos jurídicos se apresentam sobretudo por meio de formas representativas escritas, as quais tem o seu significado extraído pelo intérprete pela reconstrução da experiência do outro sujeito em um cenário em que estão presentes conceitos familiares e contemporâneos à experiência do próprio intérprete (ARANHA e OLIVEIRA, 2016, p. 22). Essa ideia está além da noção mais simplista de transpor um significado antigo da forma representativa

para o presente (ARANHA e OLIVEIRA, 2016, p. 22). Por isso, no âmbito da hermenêutica prescritiva, é importante que o intérprete tenha conhecimento da matéria que interpretará (ARANHA e OLIVEIRA, 2016, p. 22).

Desse modo, pode-se dizer que a interpretação técnico-jurídica se preocupa com a formação de conceitos coerentemente organizados com o propósito de alcançar uma definição mais precisa de uma instituição jurídica quando interdisciplinarmente utilizada. Para cumprir com este fim, o intérprete adota conceitos-chave ou tipos ideais que passam a funcionar como apoio para a reconstituição atual do significado da forma representativa produzida no passado. No Modelo TLICS, exemplo de tipo ideal para interpretação de instituições jurídicas (ARANHA e OLIVEIRA, 2016, p. 22) é a categoria de "garantia institucional" (ARANHA e OLIVEIRA, 2016, p. 22), a qual será melhor explorada no tópico 1.2.1.4.

Atualmente, a pesquisa comparativa em TIC enfrenta dificuldades em realizar o seu propósito por causa do uso demasiado de tipos-ideias de conceito abrangente para a interpretação de variáveis institucionais, como, por exemplo, as definições de separação de poderes e federalismo. No modelo TLICS, no entanto, o que se busca é utilizar tipos-ideias de conceitos menos abrangentes e ambíguos, de forma que seus significados fiquem melhor preservados ao longo do tempo (ARANHA e OLIVEIRA, 2016, p. 22).

A metodologia hermenêutica de Betti apresentou algumas diretrizes para orientar o processo interpretativo, organizando-as em 4 cânones (ARANHA e OLIVEIRA, 2016, p. 22), os quais formam um conjunto carregado de complementariedade e correção recíproca (SPAREMBERGER, 2003, p. 181).

O primeiro, chamado cânone da autonomia hermenêutica do objeto (*sensus non est inferendus sed efferendus*), determina que o significado deve ser extraído da forma representativa e, não, inferido aleatoriamente (ARANHA e OLIVEIRA, 2016, p. 22). Isso porque, as formas representativas são a objetivação da espiritualidade de um outro sujeito, sendo autônomas em seu sentido e impondo subordinação ao sujeito que as interpreta (PESSÔA, 2002, p. 107).

O segundo cânone é o da coerência do sentido ou do princípio da totalidade (ARANHA e OLIVEIRA, 2016, p. 22). Segundo Betti, apesar de as formas representativas serem objetivações de um outro sujeito, elas apresentam

apenas aspectos parciais dessa espiritualidade que as gerou (PESSÔA, 2002, p. 107-108). Entretanto, ainda assim, o espírito gerador deve ser conhecido como o todo que é, não sendo suficiente apenas o conhecimento de seus aspectos parciais presentes na forma representativa (PESSÔA, 2002, p. 108). Em outras palavras, Betti estabelece que o sentido do todo deve ser entendido a partir de seus elementos individuais e o elemento individual deve ser entendido em relação ao todo do qual faz parte (ARANHA e OLIVEIRA, 2016, p. 22-23). Esse cânone se refere a uma exigência da hermenêutica clássica, resgatada por Schleiermacher, e que ficou conhecida como círculo hermenêutico (SPAREMBERGER, 2003, p. 179). Segundo essa ideia, a compressão do texto se daria pelo contexto, a partir da iluminação recíproca das partes em relação ao todo e do todo em relação às partes (SPAREMBERGER, 2003, p. 179).

O terceiro cânone, o da atualidade do entendimento, se preocupa em elucidar o primeiro cânone ao estabelecer que a busca pela objetividade não pode ser confundida com a exclusão do intérprete do processo hermenêutico, na medida em que se espera que os próprios objetos falem por si (PESSÔA, 2002, p. 110). Assim, a fim de exercer o seu papel, o intérprete deve refazer o processo criativo segundo a sua qualidade intelectual e de acordo com as suas próprias experiências (ARANHA e OLIVEIRA, 2016, p. 23). Desse modo, uma vez que no processo interpretativo a subjetividade está presente, um espírito ou um sujeito fala ao outro através da forma representativa, de modo que o espírito do intérprete, ao receber a mensagem, se sente impulsionado a se voltar para essa forma representativa e inquiri-la acerca do seu significado (SPAREMBERGER, 2003, p. 180). Como consequência da responsabilidade do intérprete de refazer o processo criativo, se torna imprescindível uma formação jurídica comum entre aqueles que analisam estruturas legais e regulatórias (ARANHA e OLIVEIRA, 2016, p. 23). Ainda de acordo com o jurista italiano, a variação histórica das interpretações se explica em função da influência da subjetividade no processo interpretativo (SPAREMBERGER, 2003, p. 180). O que se conclui é que a interpretação não é uma tarefa definitiva, mas sempre inconclusa e, por isso, constante (SPAREMBERGER, 2003, p. 180).

Se, no terceiro cânone, o autor destaca a participação do sujeito no processo interpretativo, no quarto e último cânone, Betti a limita, a fim afastar o

arbítrio da subjetividade, que é justamente o que os dois primeiros cânones também buscavam fazer (PESSÔA, 2002, p. 110).

O quarto cânone é o da correspondência hermenêutica de significado ou adequação de significado na compreensão, segundo o qual o intérprete deve, do ponto de vista positivo, buscar a harmonia entre o estímulo que recebe da forma representativa e a sua própria atualidade (ARANHA e OLIVEIRA, 2016, p. 23), e deve, do ponto de vista negativo, se resguardar de pré-julgamentos (PESSÔA, 2002, p. 111). Conclui-se, assim, que, no processo interpretativo, deve haver certo nível de concordância entre intérprete e interpretado (SPAREMBERGER, 2003, p. 181).

1.2.1.2. A hermenêutica concreta de Hesse no Modelo TLICS

O Modelo TLICS adotou o método interpretativo de concretização proposto por Konrad Hesse (1919-2005) como metodologia específica para a interpretação de princípios constitucionais e estruturais do Estados, além de direitos fundamentais (ARANHA e OLIVEIRA, 2016, p. 24).

Segundo o autor alemão, o método concretista de interpretação tem três pilares, quais sejam, a norma que vai se concretizar, a compreensão prévia do intérprete e o problema concreto que deve se resolver (FONSECA, 2005, p. 168). Assim, de acordo com essa metodologia interpretativa, a norma somente adquire significado com a concretização, ou seja, com a sua aplicação ao caso concreto, canalizando-se em um processo único a interpretação e a aplicação normativas (FONSECA, 2005, p. 168). Além disso, o entendimento de normas e princípios constitucionais depende de sua aplicação infinita em casos concretos, o que faz com que o significado das formas representativas esteja sempre alinhado com os limites dos significados das declarações escritas (ARANHA e OLIVEIRA, 2016, p. 24). Assim, pode-se afirmar que Hesse se afasta de tendências hermenêuticas segundo as quais a interpretação da norma abstrata e a aplicação da mesma ao caso concreto constituem momentos separados e distintos (FONSECA, 2005, p. 168).

Além disso, para o autor, o texto jurídico a ser concretizado deve ser compreendido, sem que esse entendimento se afaste nem da pré-compreensão do intérprete, nem do caso concreto (STRECK, 2001, p. 244). Ou seja, aquele que interpreta não pode extrair o conteúdo da norma fora do seu próprio contexto

histórico, o qual moldou seus conhecimentos e pré-juízos (STRECK, 2001, p. 244).

Friedrich Müller (1938 – atualmente) adiciona à teoria de Hesse o conceito de norma de decisão (*Entscheidungsnorm*), a qual funciona como um limite para a transformação do significado da norma através do processo infinito de concretização (ARANHA e OLIVEIRA, 2016, p. 24). A norma de decisão também funciona como um tipo ideal para a interpretação (ARANHA e OLIVEIRA, 2016, p. 24). Hesse e Müller reconhecem o processo interpretativo como sendo um processo contínuo que faz a comunicação entre o texto jurídico e o contexto (ARANHA e OLIVEIRA, 2016, p. 24).

1.2.1.3. A teoria institucional do direito de Santi Romano no Modelo TLICS

O modelo TLICS tem, entre suas duas teorias de suporte, a teoria institucional do direito (ARANHA e OLIVEIRA, 2016, p. 24). Essa corrente dispõe direitos subjetivos e objetivos como parte do mesmo fenômeno, a partir de uma perspectiva institucional (ARANHA e OLIVEIRA, 2016, p. 24).

Segundo a teoria institucional do direito, os textos jurídicos não são a Lei em si, mas, sim, expressões que compõem um quadro jurídico (ARANHA e OLIVEIRA, 2016, p. 24). Este quadro, por sua vez, é definido como o corpo institucional que produz a lei, se comportando como um organismo vivo e dinâmico que é influenciado pelos próprios textos jurídicos e que, ao mesmo tempo, os influencia (ARANHA e OLIVEIRA, 2016, p. 24). Importa observar que, para o autor, o quadro jurídico, sendo um corpo institucional, é composto por aspectos institucionais, como o legislativo, o executivo e o judiciário (ARANHA e OLIVEIRA, 2016, p. 24).

Como consequência dessas ideias, tem-se que o significado das declarações jurídicas singulares depende do contexto institucional no qual se encontram, ainda que apresentem um sentido literal (ARANHA e OLIVEIRA, 2016, p. 24). Isto é, como a teoria institucional do direito tem fundamentos tanto objetivos quanto subjetivos (ARANHA e OLIVEIRA, 2016, p. 25), pode-se dizer que a interpretação de uma certa declaração jurídica depende de uma lógica institucional de princípios, e, não, simplesmente, de seu texto ou de seu conteúdo moral subjetivo (ARANHA e OLIVEIRA, 2016, p. 24-25).

Por fim, a teoria institucional afirma que existe uma pluralidade de tipos-ideias no contexto institucional do direito e que, para elucidar quais seriam esses tipos-ideias, deve se utilizar dos meios oferecidos pela própria teoria, a exemplo das trazidas pela teoria das garantias institucionais (ARANHA e OLIVEIRA, 2016, p. 25).

1.2.1.4. A teoria das garantias institucionais de Carl Schmitt no Modelo TLICS

Segundo a teoria das garantias institucionais de Carl Schmitt (1888-1985), os conceitos jurídicos extraem o seu sentido das garantias institucionais que estão atomizadas em uma estrutura jurídica (ARANHA e OLIVEIRA, 2016, p. 25).

Apesar de comumente serem citados pelo termo genérico de garantias institucionais, os mais importantes conceitos dessa teoria são os de garantias institucionais (*institutionelle Garantien*) e garantias do instituto (*Institutsgarantien*) (ARANHA e OLIVEIRA, 2016, p. 25).

As garantias do instituto estão conectadas a instituições jurídicas de caráter subjetivo, a exemplo dos direitos fundamentais. Pode-se dizer que o significado de uma garantia do instituto depende mais da cultura e da tradição jurídica de um determinado contexto do que das declarações de uma estrutura jurídica (ARANHA e OLIVEIRA, 2016, p. 25).

As garantias institucionais, por sua vez, dizem respeito às instituições jurídicas relacionadas à estrutura jurídica. Quanto ao seu significado, este será melhor assegurado quando positivado na lei (ARANHA e OLIVEIRA, 2016, p. 25).

Em suma, é possível afirmar que o primeiro conceito tem natureza pública e o segundo, privada. Essa diferenciação é relevante para a construção de uma metodologia de estudo comparado que compreenderá uma determinada variável por meio de sub-blocos atomizados, tal qual se pretende realizar com o Modelo TLICS. Isso porque, esses dois conceitos prevenirão que uma declaração escrita seja entendida da mesma forma em contextos diferentes, ou seja, em tradições jurídicas distintas (ARANHA e OLIVEIRA, 2016, p. 25).

Em resumo, o modelo TLICS utiliza blocos de atributos jurídicos complexos, o quais podem ser analisados de forma desassociada ou como um conjunto de garantias conectadas entre si (ARANHA e OLIVEIRA, 2016, p. 26).

Como consequência, a viabilidade de se estudar tanto garantias individuais quanto variáveis jurídicas complexas possibilita a pesquisa comparativa em diversos formatos, como, por exemplo, na comparação de variáveis específicas entre dois países ou até mesmo no uso de variáveis de maior estatura na estrutura jurídica, como direitos fundamentais e princípios constitucionais, entre os quais se encontra a garantia de proteção de dados pessoais (ARANHA, MENDES, *et al.*, 2019, p. 143).

1.2.2. O modelo TLICS e seus indicadores para proteção de dados pessoais

Após a análise das teorias que apoiam o Modelo TLICS genericamente considerado, parte-se, neste tópico, para a compreensão das variáveis jurídicas pertencentes ao método quando aplicado a estudos comparados em direito de proteção de dados pessoais. Essas variáveis foram elaboradas no trabalho de Aranha, Mendes, et al. (2020), segundo o qual, as estruturas jurídicas referentes à matéria de proteção de dados podem ser atomizadas em 6 formas institucionais, divididas em 28 instituições legais e 51 subtipos de instituições legais. Além disso, essas variáveis podem ser avaliadas tanto de um ponto de vista qualitativo, quanto quantitativo (ARANHA, MENDES, *et al.*, 2020). Reitera-se que o objetivo é traçar um quadro das estruturas jurídicas de proteção de dados pessoais do Brasil, do Japão e da Coreia do Sul, o qual, a partir da aplicação do Modelo TLICS poderá ser analisado por meio de blocos de atributos jurídicos complexos tomados separadamente ou em conjunto.

De forma prática, esse trabalho comparará a estrutura jurídica de cada país de acordo com as 6 formas institucionais e as 28 instituições jurídicas organizadas na Tabela 1:

Formas Institucionais	Instituições jurídicas
Entidade Jurídica	Autoridade de Proteção de Dados
	Conselho de Proteção de Dados
Qualidade Jurídica	Titulares de Dados
	Operador

	Controlador
	Órgão de Pesquisa
	Encarregado
Objeto Jurídico	Dados Pessoais
	Dados Pessoais Sensíveis
	Banco de Dados
	Avaliação de Impacto
	Âmbito Territorial
	Âmbito Material
Status Jurídico	Fundamentos Jurídicos para o Tratamento de Dados Pessoais
	Fundamentos Jurídicos para o Tratamento de Dados Pessoais Sensíveis
	Dado Anonimizado, Bloqueado ou Apagado
Relação Jurídica entre Sujeitos	Transferência Internacional de Dados ou Processamento Transfronteiriço
	Uso Compartilhado de Dados Pessoais
	Responsabilidade e Ressarcimento de Danos
	Sanções Administrativas
Relação Jurídica entre Sujeito e Objeto	Tratamento de Dados
	Tratamento de Dados Sensíveis
	Tratamento de Dados de Crianças e Adolescentes
	Tratamento de Dados por Autoridades Públicas
	Anonimização
	Obrigações do Controlador de Dados
	Mecanismos de Governança e de Prestação de Contas

Tabela 1 – Formas institucionais e instituições legais de proteção de dados pessoais, conforme o Modelo TLICS.

CAPÍTULO 2: Aspectos convergentes e divergentes entre a Lei sobre a Proteção de Informações Pessoais do Japão e a Lei de Proteção de Informações Pessoais da Coreia do Sul

1. Questões preliminares

Antes de se realizar as análises as quais se prestam o segundo e o terceiro capítulo deste trabalho, é necessário elucidar algumas questões.

O segundo capítulo desta monografia se debruçará sobre a identificação dos aspectos convergentes e divergentes entre as leis do Japão e da Coreia do Sul para proteção de dados pessoais (a APPI e a PIPA, respectivamente). Essa análise tem o propósito didático de, por meio da comparação, apresentar esses dois arcabouços jurídicos ao leitor.

O terceiro e último capítulo, por sua vez, se preocupará em analisar os aspectos convergentes e divergentes entre a lei brasileira e japonesa (a LGPD e a APPI, respectivamente) e entre a lei brasileira e coreana (a LGPD e a PIPA, respectivamente), com o propósito de compreender se a proteção de dados pessoais oferecida pela APPI e pela PIPA tem níveis semelhantes à oferecida pela LGPD e se, portanto, a transferência de dados pessoais entre o Brasil e os dois países asiáticos se realizaria sem prejuízo dos direitos dos titulares.

Conforme se explicou no tópico 1.2.2 do Capítulo 1, o Modelo TLICS apresenta 6 formas institucionais, divididas em 28 instituições jurídicas, as quais, por sua vez, se decompõem em 51 subtipos diferentes. Essa estrutura permite que regramentos jurídicos sejam detalhados em categorias, as quais podem ser facilmente cotejadas para análise de seus conteúdos, constituindo ferramenta ideal para estudos comparados. Por isso, a LGPD, a APPI e a PIPA foram destrinchadas em uma tabela que contém todos os 51 subtipos de instituições jurídicas do Modelo TLICS no Anexo I, ao final do trabalho.

No entanto, para a identificação dos aspectos convergentes e divergentes e o reconhecimento da existência ou não de comensurabilidade de proteção de dados pessoais entre a LGPD e a APPI e entre a LGPD e a PIPA (a serem desenvolvidos nos Capítulos 2 e 3), se optou por evidenciar 18 dos 51 subtipos de instituições jurídicas presentes no Modelo TLICS. O motivo dessa escolha é o de apresentar as variáveis mais representativas em formato passível de compreensão quando da comparação de três leis diferentes. Contudo, salienta-

se que, da opção por se utilizar um número menor de variáveis, não decorre prejuízo, tendo em vista constituírem os parâmetros mais básicos de proteção de dados pessoais a ser conferidos por leis e regulamentos, como recorte voltado a evidenciar três apresentações institucionais da proteção de dados: a apresentação institucional da autoridade de proteção de dados pessoais, o elenco de direitos e a transferência internacional de dados. Essas 18 espécies se encaixam, portanto, em três categorias principais, a saber: autoridade de proteção de dados, direitos individuais dos titulares e hipóteses de transferência internacional de dados.

Por fim, importa explicar que, ao longo da análise, poderá ser mencionada a sigla PIHBO, no âmbito da lei japonesa de proteção de dados. Esse termo é o acrônimo em inglês para "*Personal Information Handling Business Operator*", figura semelhante ao controlador de dados presente no RGPD (TAKASE, 2017) e, também, na LGPD. Se optou pelo uso do acrônimo em inglês para simplificar a citação do termo nas tabelas.

2. Aspectos convergentes e divergentes entre a APPI e a PIPA

As variáveis jurídicas selecionadas serão abordadas comparativamente nos tópicos seguintes. As mesmas podem ser visualizadas de forma geral na tabela abaixo.

Formas Institucionais	Instituições Jurídicas	Subtipo de Instituição Jurídica
Entidade Jurídica	Autoridade de Proteção de Dados	Autônoma/Independente
		Apresentação Federativa
Qualidade Jurídica	Titulares de Dados	Definição
		Direito de Ser Informado
		Direito de Acesso
		Direito à Retificação
		Direito ao Esquecimento ou Direito ao Apagamento
		Direito à Revogação
		Direito à Limitação do Tratamento

		Direito de Portabilidade dos Dados
		Direito a Bloqueio ou Restrição do Processamento
		Direito à Intervenção Humana na Tomada de Decisão e Criação de Perfil Automatizadas
		Limitações
Relação Jurídica entre Sujeitos	Transferência Internacional de Dados ou Processamento Transfronteiriço	Decisão de Adequação
		Consentimento
		Contrato
		Regras Vinculativas Aplicáveis às Empresas
		Certificados e Códigos de Conduta

Tabela 2 – Formas institucionais, instituições legais e seus subtipos selecionados para análise da comensurabilidade entre as leis de proteção de dados do Brasil, do Japão e da Coreia do Sul.

- **Quanto à entidade jurídica**

2.1. Autoridade de proteção de dados

As autoridades de proteção de dados no Japão e na Coreia do Sul são chamadas “Comissão de Proteção de Informações Pessoais”, sendo mencionadas ao longo dos textos normativos apenas como “Comissão” na APPI e como “Comissão de Proteção” na PIPA.

2.1.1. Autônoma/Independente

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**APPI (Japão)**	**PIPA (Coreia do Sul)**
Autoridade de Proteção de Dados	Autônoma/ Independente	Artigo 59 (nº2) e artigo 62: "(2) A Comissão pertence à jurisdição do Primeiro Ministro"; "O presidente e os comissários da Comissão devem exercer a sua autoridade oficial de forma independente".	Artigo 7º (nº1) e (nº2): "(1) A Comissão de Proteção de Informações Pessoais (doravante referida como a "Comissão de Proteção") será estabelecida pelo Primeiro-Ministro para conduzir de forma independente o trabalho relacionado com a

			proteção de informações pessoais. (2) A Comissão de Proteção será considerada uma agência administrativa central nos termos do Artigo 2 da Lei de Organização do Governo (...)"

Tanto o Japão quanto a Coreia do Sul têm autoridade de proteção de dados com exercício independente de suas funções.

A alteração da APPI que foi promovida em 2015 foi responsável pela criação da chamada Comissão de Proteção de Informações Pessoais, uma autoridade de controle independente, responsável pela supervisão e aplicação coerciva da referida lei (EUROPEIA, 2019a, p. 3). A mais recente emenda à APPI, promulgada em 12 de junho de 2020, não trouxe alterações quanto a esse quesito.

Em relação à Coreia do Sul, entrou em vigor, no dia 05 de agosto de 2020, a mais recente emenda à PIPA, trazendo mudanças importantes (WHON-IL, 2020). Dentre elas está a reestruturação administrativa da supervisão da proteção de dados no país, que ocorreu com o intuito de melhor atender aos padrões do RGPD, visando decisão de adequação posterior favorável por parte da Comissão Europeia (KWANG HYUN RYOO, 2020). Com isso, se antes a autoridade para proteção de dados estava dividida entre o Ministro do Interior e Segurança e a Comissão de Comunicações da Coreia (acrônimo em inglês KCC), agora essa tarefa é de atribuição da Comissão de Proteção de Informações Pessoais (KWANG HYUN RYOO, 2020). Desse modo, a Comissão de Proteção passou a ser um órgão regulador independente, com poderes para monitorar e policiar a privacidade de informações pessoais (KWANG HYUN RYOO, 2020).

2.1.2. Apresentação Unitária

Instituição Jurídica	Subtipo de Instituição Jurídica	APPI (Japão)	PIPA (Coreia do Sul)

Autoridade de Proteção de Dados	Apresentação Unitária	Artigo 59 (nº2): "(2) A Comissão pertence à jurisdição do Primeiro-Ministro.";	Artigo 7º (nº1) e (nº2): "(1) A Comissão de Proteção de Informações Pessoais (doravante referida como a "Comissão de Proteção") será estabelecida pelo Primeiro-Ministro para conduzir de forma independente o trabalho relacionado com a proteção de informações pessoais. (2) A Comissão de Proteção será considerada uma agência administrativa central nos termos do Artigo 2 da Lei de Organização do Governo (...)"

A organização da Autoridade Nacional de Proteção de Dados tanto no Japão quanto na Coreia do Sul é unitária e, não, federativa. Isso porque a atividade de controle de proteção está centrada em suas respectivas Comissões.

É o que se extrai do art. 59 (nº2) da APPI, segundo o qual a Comissão, ainda que independente, pertence à jurisdição do Primeiro Ministro, que é nacional. No mesmo sentido, a PIPA informa no art. 7º (nº1) que a Comissão independente é estabelecida pelo Primeiro Ministro. De forma ainda mais patente, o art. 7º (nº2) do mesmo diploma afirma que o órgão de controle é uma agência administrativa central.

- **Quanto à qualidade jurídica**

2.2. Titulares de Dados

2.2.1. Definição

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**APPI (Japão)**	**PIPA (Coreia do Sul)**
Titulares de Dados	Definição	Artigo 2º (nº 8): "(8) Um 'titular' de informações pessoais, nesta Lei, significa um indivíduo	Artigo 2º (nº3): "3. O termo 'titular dos dados' significa um indivíduo que é identificável por meio das

		específico identificável por informações pessoais"	informações processadas e é o sujeito dessas informações;"

No Japão, se designa o titular de dados apenas como “titular” e, na Coreia do Sul, como “titular dos dados”.

A semelhança mais importante é a de que, nos dois casos, o titular de dados deve ser pessoa identificável e, não necessariamente, pessoa identificada. Sendo assim, a proteção dos dados também abrange indivíduos que passarem a ser identificados mediante emprego de esforço razoável. Os parâmetros, no entanto, de que empenho seja esse, são definidos de forma específica em cada legislação.

Segundo a Comissão de Proteção de Informações Pessoais do Japão, o indivíduo identificável é aquele cujas informações, quando cotejadas com outras, permitem identificar determinada pessoa singular (EUROPEIA, 2019a, p. 4). A avaliação sobre se as informações podem ser consideradas cotejáveis será realizada caso a caso, levando em consideração se o referido recolhimento puder ser realizado por um controlador médio recorrendo aos meios que lhe estão disponíveis (EUROPEIA, 2019a, p. 4).

Na Coreia do Sul, por sua vez, o critério para definir um dado pessoal tem sentido semelhante ao mencionado acima. Conforme o art. 2º (nº1; b) da PIPA, o termo “informações pessoais” significa, dentre outras definições, informações que, mesmo que por si só não identifiquem um determinado indivíduo, podem ser facilmente combinadas com outras para identificá-lo (KWANG BAE PARK, 2020). O grau de facilidade para tal é elucidado no mesmo dispositivo: se há ou não facilidade de combinação deve ser determinado considerando razoavelmente o tempo, custo, tecnologia, etc. usados para identificar o indivíduo, assim como a probabilidade de que outras informações possam ser obtidas (KWANG BAE PARK, 2020).

O que se conclui é que, pelo fato da APPI e da PIPA considerarem como titular de dados pessoais tanto pessoa identificada, quanto pessoa identificável, a proteção conferida por essas leis é mais abrangente. Nesse sentido, ambas as legislações apresentam uma ótica expansionista (em antagonismo à ótica reducionista) ao resguardar os direitos dos indivíduos (BIONI, 2020, p. 58-59).

2.2.2. Direito de ser informado

Instituição Jurídica	Subtipo de Instituição Jurídica	APPI (Japão)	PIPA (Coreia do Sul)
Titulares de Dados	Direito de Ser Informado	Artigo 27 (nº1; i a iv): "(1) Um PIHBO, em relação às informações pessoais retidas por si, disponibilizará os tópicos descritos a seguir de forma que o titular possa conhecê-los (incluindo aqueles casos em que, a pedido de um titular, responderá sem demora).	Artigo 4 (nº1): "O titular dos dados tem os seguintes direitos em relação ao tratamento das suas próprias informações pessoais: 1. O direito de ser informado sobre o processamento de tais informações pessoais;"

O titular de dados tem o direito de ser informado nos dois países, de modo que as principais características do processamento de suas informações lhe devem ser comunicadas.

Dentre essas características, a que mais se destaca é comunicação da finalidade do processamento dos dados pessoais, dever do controlador previsto tanto na APPI quanto na PIPA. O art. 27 (nº1; ii) da APPI estabelece que o PIHBO disponibilizará, de forma que o titular possa conhecer, dentre outros tópicos, a finalidade de utilização de seus dados pessoais retidos (com algumas exceções). Também a PIPA, no art. 15 (nº2; 1), menciona que o controlador de informações pessoais deve informar ao titular dos dados, dentre outros itens, quando obtiver o seu consentimento, a finalidade da coleta e do uso de suas informações pessoais.

2.2.3. Direito de Acesso

Instituição Jurídica	Subtipo de Instituição Jurídica	APPI (Japão)	PIPA (Coreia do Sul)
Titulares de Dados	Direito de Acesso	Artigo 28 (nº1): "(1) Um titular pode exigir de um PIHBO a divulgação de dados pessoais retidos que possam identificar ele ou ela por um método de fornecimento de registro	Artigo 4 (nº3): "O titular dos dados tem os seguintes direitos em relação ao tratamento das suas próprias informações pessoais:

		eletromagnético ou outros métodos prescritos pelas regras da Comissão de Proteção de Informações Pessoais."	3. O direito de confirmar se as informações pessoais estão ou não sendo processadas e de solicitar acesso (incluindo o fornecimento de cópias; doravante o mesmo se aplica) a essas informações pessoais;"

Em ambos os países o titular de dados tem o direito de acessar quais de suas informações pessoais estão sendo processadas.

Importa destacar a ampliação desse direito trazida pela emenda de 2020 à APPI (Japão), por meio de duas mudanças.

A primeira foi a permissão de que os dados mantidos por um controlador sejam fornecidos ao titular em formato eletrônico. Antes, a divulgação era atendida por meio de documentos impressos, como regra (CHANCE, 2020, p. 2).

A segunda diz respeito ao alargamento do escopo do que sejam “dados pessoais retidos” e, como consequência, do direito de acesso dos titulares. Conforme a nova redação do art. 2º (nº7) da APPI, a expressão “dados pessoais retidos” abrange os dados pessoais que um PIHBO tem autoridade para divulgar, corrigir, adicionar ou excluir o conteúdo, cessar a utilização, apagar e cessar o fornecimento a terceiros. Antes da emenda, a redação do artigo tinha uma acréscimo, de forma que, dados que de maneira pré-determinada fossem excluídos em 6 meses a partir da sua aquisição constituíam uma exceção ao conceito de “dados pessoais retidos” e, portanto, uma exceção à aplicação das ações mencionadas acima (CHANCE, 2020, p. 2). Assim, com o novo texto, todos os dados pessoais, independentemente do período de retenção, devem ser qualificados como retidos, e, portanto, disponibilizados conforme requerimento do titular (CHANCE, 2020, p. 2).

Quanto a esse segundo avanço, é possível concluir ainda que, assim como o direito de acesso foi expandido, o mesmo ocorreu com o direito à retificação (tópico 2.2.4), à limitação do tratamento (tópico 2.2.7) e ao bloqueio ou restrição do processamento (tópico 2.2.9), tendo em vista que o art. 2º (nº7) da APPI também fala em correção, adição e exclusão de conteúdo e cessação de utilização e de fornecimento a terceiros.

2.2.4. Direito à Retificação

Instituição Jurídica	Subtipo de Instituição Jurídica	APPI (Japão)	PIPA (Coreia do Sul)
Titulares de Dados	Direito à Retificação	Artigo 29 (nº1): "(1) Um titular pode, quando o conteúdo de dados pessoais retidos que podem identificá-lo não estiver exato, exigir que um PIHBO faça uma correção, adição ou exclusão (de agora em diante denominada "correção etc." no presente artigo) em relação ao conteúdo dos dados pessoais retidos."	Artigo 4 (nº4): "O titular dos dados tem os seguintes direitos em relação ao tratamento das suas próprias informações pessoais: 4. O direito de suspender o processamento e solicitar a correção, exclusão e destruição de tais informações pessoais;"

Conforme é possível verificar, o direito à retificação é garantido de forma ampla aos titulares de dados tutelados pela APPI e pela PIPA. Nos dois casos, um indivíduo pode exigir que suas informações não exatas ou incorretas sejam corrigidas.

2.2.5. Direito ao Esquecimento ou Direito ao Apagamento

Instituição Jurídica	Subtipo de Instituição Jurídica	APPI (Japão)	PIPA (Coreia do Sul)
Titulares de Dados	Direito ao Esquecimento ou Direito ao Apagamento	Não há previsão legal	Artigo 36 (nº1): "(1) Um titular de dados que tenha acessado suas informações pessoais nos termos do Artigo 35 pode solicitar uma correção ou apagamento de tais informações pessoais ao controlador de informações pessoais relevante: Dado que o apagamento não é permitido quando as referidas informações pessoais forem recolhidas por outros estatutos."

O termo direito ao esquecimento (do inglês, “*right to be forgotten*”) não tem menção explícita em nenhum dos arcabouços jurídicos. Porém, a terminologia direito ao apagamento (do inglês, “*right to erasure*”) se apresenta de forma mais evidente no art. 36 (nº1) da PIPA, denominado, em inglês, “*rectification or erasure of personal information*”, o qual garante, em regra, o direito ao titular de apagar seus dados pessoais de forma ampla.

Ainda assim, a seguir, se analisará o que seja o direito ao esquecimento e ao apagamento para que melhor se compreenda a definição da presença ou não dessas garantias no arcabouço jurídico japonês e coreano.

Os termos esquecimento e apagamento rementem diretamente ao art. 17 do Regulamento Geral sobre Proteção de Dados (RGPD), intitulado “Direito ao apagamento dos dados (direito de ser esquecido)”. Segundo esse excerto, o titular tem o direito de obter o apagamento de seus dados, sem demora injustificada, por parte do responsável pelo tratamento. Esse comando aproxima, portanto, o direito ao esquecimento do direito ao apagamento.

O entendimento acima é ratificado pelo Considerando 66 do RGPD, que assevera que o direito ao esquecimento, no ambiente eletrônico, deve ser reforçado através do alargamento do direito ao apagamento, inclusive mediante a comunicação aos responsáveis pelo tratamento de dados pessoais de que os titulares solicitaram a supressão de quaisquer ligações para esses dados pessoais ou de cópias ou reproduções dos mesmos (EUROPEU, 2016).

No entanto, se de um lado, o direito europeu considera o direito ao esquecimento e ao apagamento espécies aproximadas, por outro, no âmbito doutrinário, esses são direitos autônomos (LIMA e RAMIRO, 2020, p. 261). A seguinte análise serve, dessa forma, para entender se a presença do direito ao apagamento em um ordenamento jurídico é suficiente para se falar em direito ao esquecimento também, como se os dois fossem termos intercambiáveis.

Primeiramente, segundo a doutrina, o direito ao esquecimento é autônomo, e não se confunde com privacidade, nem com identidade pessoal (LIMA e RAMIRO, 2020, p. 261). Essencialmente, pode ser definido como o direito de ser deixado em paz e recair no anonimato para que não seja relembrado a todo momento de fatos que almeja deixar no passado, a fim de que não lhe causem mais constrangimentos, permitindo que uma pessoa exerça a possibilidade de ser a si mesmo (LIMA e RAMIRO, 2020, p. 264).

O destaque direcionado à discussão do que seja o direito ao esquecimento surgiu em função do poder de eternização e facilitação de acesso da informação pela internet, independentemente do lapso temporal havido entre o acontecimento e a sua disponibilização (LIMA e RAMIRO, 2020, p. 264).

O direito ao esquecimento, portanto, parece ser distinto do direito ao apagamento, na medida em que, nem sempre quando se visa efetivar o primeiro, se busca a eliminação de todas as fontes primárias do evento ou de todos os dados relacionados (LIMA e RAMIRO, 2020, p. 264). O objetivo é que determinado evento não seja resgatado, levando-se em consideração a ausência de interesse público e o lapso temporal entre o acontecimento e a transmissão de informações sobre o fato (LIMA e RAMIRO, 2020, p. 264). O próprio Considerando 66 do RGPD parece sugerir que o direito ao apagamento pode ser usado como um instrumento para se atingir o direito autônomo ao esquecimento.

O direito ao apagamento, desse modo, parece ter aplicação mais ampla, apesar de admitir exceções, como o art. 36 (nº1) da PIPA, que não consente no apagamento de dados recolhidos com base em outros estatutos.

O que se conclui é que, apesar de a PIPA oferecer aos seus titulares o direito ao apagamento, não se pode falar que garanta também o direito ao esquecimento.

Quanto à APPI, apesar de apresentar no art. 30 (denominado “Cessação de utilização, etc.”) termo que denota apagamento (do inglês, “*deletion*”), não permite ao titular promover a eliminação de seus dados de maneira tão ampla quanto a PIPA, não podendo se falar, assim, em direito de apagamento. Também não há menção ao direito ao esquecimento no âmbito japonês.

É o que se extrai da redação do art. 30 (nºs 1 e 5) da APPI. Segundo os dispositivos, o titular só pode exigir que um controlador cesse a utilização ou elimine seus dados pessoais quando essas informações: (i) forem usadas para uma finalidade diferente da originalmente notificada; (ii) forem adquiridas por engano ou meios impróprios; (iii) forem utilizadas de forma ilegal ou injusta; (iv) não forem mais necessárias ao controlador; (v) vazarem acidentalmente; (vi) se tratadas, puderem prejudicar os direitos ou interesses legítimos do titular (CHANCE, 2020, p. 2).

2.2.6. Direito à Revogação

Instituição Jurídica	Subtipo de Instituição Jurídica	APPI (Japão)	PIPA (Coreia do Sul)
Titulares de Dados	Direito à Revogação	Artigo 30 (nº1) e (nº5): "(1) Um titular pode, quando dados pessoais retidos que possam identificá-lo estão sendo tratados em violação às disposições do Artigo 16 ou Artigo 16-2, ou, foram adquiridos em violação às disposições do Artigo 17, exigir de um PIHBO a cessação da utilização ou eliminação (doravante referida como “cessação da utilização etc.” neste Artigo) dos dados pessoais retidos."; "(5) Um titular pode exigir que o PIHBO cumpra uma cessação de utilização etc. dos dados pessoais retidos, ou cesse uma provisão a terceiros, se tiver se tornado desnecessário para o PIHBO utilizar dados pessoais retidos que possam identificar o titular, se uma situação prescrita na cláusula principal do Artigo 22-2, parágrafo (1) ocorreu em conexão com os dados pessoais retidos que possam identificar o titular, ou existe a possibilidade de que o tratamento dos dados pessoais retidos que possam identificar o titular prejudiquem os direitos ou interesses legítimos desse."	Artigo 4 (nº4): "O titular dos dados tem os seguintes direitos em relação ao tratamento das suas próprias informações pessoais: 4. O direito de suspender o processamento e solicitar a correção, exclusão e destruição de tais informações pessoais;"

O direito de revogação (do inglês “*right to cancel*”) tutela o poder do titular de revogar seu consentimento ou cancelar o processamento de seus dados por meio da eliminação desses. Pelo menos em relação ao segundo aspecto, a eliminação, existe previsão legal tanto na PIPA, quanto na APPI.

Conforme já mencionado no tópico anterior, o art. 30 (nºs 1 e 5) da APPI concede ao titular o direito de exigir do controlador a eliminação de dados empregados em finalidade diferente da originária, adquiridos ou utilizados impropriamente, desnecessários ao controlador, acidentalmente vazados ou prejudiciais aos interesses legítimos do titular, caso tratados.

A PIPA, no mesmo sentido, em seu art. 4º (nº4) garante aos indivíduos o poder de corrigir, excluir ou destruir suas informações pessoais.

No entanto, observa-se que a lei coreana é mais abrangente nas hipóteses de revogação, oferecendo o direito de maneira mais ampla que a lei japonesa.

2.2.7. Direito à Limitação do Tratamento

Instituição Jurídica	Subtipo de Instituição Jurídica	APPI (Japão)	PIPA (Coreia do Sul)
Titulares de Dados	Direito à Limitação do Tratamento	Artigo 16 (nº1), Artigo 29 (nº1) e Artigo 30 (nº1) e (nº5): "(1) Um PIHBO não deve tratar informações pessoais, sem obter previamente o consentimento do titular, para além do âmbito necessário para cumprir uma finalidade de utilização especificada de acordo com o disposto no artigo anterior."; "(1) Um titular pode, quando o conteúdo de dados pessoais retidos que podem identificá-lo não estiver exato, exigir que um PIHBO faça uma correção, adição ou exclusão (de agora em diante denominada "correção etc." no presente artigo) em relação ao conteúdo dos dados pessoais retidos."; "(1) Um titular pode, quando dados pessoais retidos que possam identificá-lo estão sendo tratados em violação às disposições do Artigo 16 ou Artigo 16-2, ou, foram	Artigo 3º (nº1) e Artigo 4º (nº4): "(1) O controlador de informações pessoais deve tornar a finalidade do processamento de informações pessoais explícita e especificada e deve coletar o mínimo de informação pessoal, legal e justamente, na medida do necessário para tal finalidade."; "O titular dos dados tem os seguintes direitos em relação ao tratamento das suas próprias informações pessoais: 4. O direito de suspender o processamento e solicitar a correção, exclusão e destruição de tais informações pessoais;"

		adquiridos em violação às disposições do Artigo 17, exigir de um PIHBO a cessação da utilização ou eliminação (doravante referida como “cessação da utilização etc.” neste Artigo) dos dados pessoais retidos."; "(5) Um titular pode exigir que o PIHBO cumpra uma cessação de utilização etc. dos dados pessoais retidos, ou cesse uma provisão a terceiros, se tiver se tornado desnecessário para o PIHBO utilizar dados pessoais retidos que possam identificar o titular, se uma situação prescrita na cláusula principal do Artigo 22-2, parágrafo (1) ocorreu em conexão com os dados pessoais retidos que possam identificar o titular, ou existe a possibilidade de que o tratamento dos dados pessoais retidos que possam identificar o titular prejudiquem os direitos ou interesses legítimos desse."	

O direito à limitação do tratamento de dados pessoais está presente tanto no arcabouço jurídico japonês quanto no coreano.

O art. 16 (nº1) da APPI e o art. 3º (nº1) da PIPA limitam o tratamento de dados pessoais ao exigir o consentimento do titular para tal atividade, além de impor que esse consentimento compreenda apenas o necessário para cumprir uma finalidade específica. A lei coreana é ainda mais explícita ao mencionar também que a coleta de informações pessoais, para a realização de uma finalidade de utilização, deva ser mínima.

Outra forma de limitar o tratamento se dá pela correção e exclusão de dados pessoais e pela suspensão do processamento ou cessação de utilização. Essas ações podem ser tomadas pelo titular com base nos arts. 29 (nº1) e 30 (nºs 1 e 5) da APPI e no art. 4º (nº4) da PIPA. Nesse caso, assim como se verificou quanto ao direito de revogação, a legislação coreana, por ser mais

genérica, é mais ampla no que diz respeito às hipóteses de evocação do direito à limitação do tratamento.

2.2.8. Direito de Portabilidade de Dados

Instituição Jurídica	Subtipo de Instituição Jurídica	APPI (Japão)	PIPA (Coreia do Sul)
Titulares de Dados	Direito de Portabilidade dos Dados	Não há previsão legal	Não há previsão legal

O direito à portabilidade de dados não encontra guarida nem no âmbito da APPI, nem no da PIPA.

2.2.9. Direito a Bloqueio ou Restrição do Processamento

Instituição Jurídica	Subtipo de Instituição Jurídica	APPI (Japão)	PIPA (Coreia do Sul)
Titulares de Dados	Direito a Bloqueio ou Restrição do Processamento	Artigo 29 (nº1) e Artigo 30 (nº1) e (nº5): "(1) Um titular pode, quando o conteúdo de dados pessoais retidos que podem identificá-lo não estiver exato, exigir que um PIHBO faça uma correção, adição ou exclusão (de agora em diante denominada "correção etc." no presente artigo) em relação ao conteúdo dos dados pessoais retidos."; "(1) Um titular pode, quando dados pessoais retidos que possam identificá-lo estão sendo tratados em violação às disposições do Artigo 16 ou Artigo 16-2, ou, foram adquiridos em violação às disposições do Artigo 17, exigir de um PIHBO a cessação da utilização ou eliminação (doravante referida como “cessação da	Artigo 4º (nº4): "O titular dos dados tem os seguintes direitos em relação ao tratamento das suas próprias informações pessoais: 4. O direito de suspender o processamento e solicitar a correção, exclusão e destruição de tais informações pessoais;"

		utilização etc.” neste Artigo) dos dados pessoais retidos."; "(5) Um titular pode exigir que o PIHBO cumpra uma cessação de utilização etc. dos dados pessoais retidos, ou cesse uma provisão a terceiros, se tiver se tornado desnecessário para o PIHBO utilizar dados pessoais retidos que possam identificar o titular, se uma situação prescrita na cláusula principal do Artigo 22-2, parágrafo (1) ocorreu em conexão com os dados pessoais retidos que possam identificar o titular, ou existe a possibilidade de que o tratamento dos dados pessoais retidos que possam identificar o titular prejudiquem os direitos ou interesses legítimos desse."	

O direito ao bloqueio ou à restrição de processamento está disponível aos titulares de dados pelas leis japonesa e coreana.

Assim, um indivíduo pode restringir ou bloquear o tratamento de seus dados de algumas formas: ao demandar a correção ou exclusão dessas informações, ou, ainda, ao pedir a suspensão do processamento ou a cessação da utilização, conforme os arts. 29 (nº1) e 30 (nºs 1 e 5) da APPI e o art. 4º (nº4) da PIPA.

Cabe ressaltar que o direito à exclusão de dados e à suspensão do processamento oferecido pela PIPA é mais abrangente que o mesmo direito previsto na APPI. A mesma reflexão foi realizada quanto ao direito à revogação, no tópico 2.6.6, e quanto ao direito à limitação do tratamento, no tópico 2.6.7.

Nesse sentido, reitera-se que o art. 4º (nº4) da PIPA prevê amplo direito à exclusão e à suspensão de processamento de dados. Mesmo quando esse dispositivo é melhor detalhado pelos arts. 36 e 37, denominados, respectivamente, “retificação ou apagamento de informações pessoais” e “suspensão do processamento de informações pessoais”, o que existem são hipóteses de exceção e, não, de aplicação da regra.

Já na APPI, ao contrário, estão previstas as hipóteses de aplicação do direito à exclusão e à suspensão. Cumpre demonstrar mais uma vez que o art. 30 (nºs 1 e 5) da APPI determina que o titular só pode exigir do controlador a eliminação e suspensão do tratamento de dados empregados em finalidade diferente da originária, adquiridos ou utilizados impropriamente, desnecessários ao controlador, acidentalmente vazados e prejudiciais aos interesses legítimos do titular, caso tratados.

2.2.10. Direito à Intervenção Humana na Tomada de Decisão e Criação de Perfil Automatizadas

Instituição Jurídica	Subtipo de Instituição Jurídica	APPI (Japão)	PIPA (Coreia do Sul)
Titulares de Dados	Direito à Intervenção Humana na Tomada de Decisão e Criação de Perfil Automatizadas	Não há previsão legal	Não há previsão legal

Ambas as leis de proteção de dados não mencionam o direito à intervenção humana na tomada de decisão e na criação de perfil automatizadas.

2.2.11. Limitações

Instituição Jurídica	Subtipo de Instituição Jurídica	APPI (Japão)	PIPA (Coreia do Sul)
Titulares de Dados	Limitações	Não há previsão legal	Artigo 58 (nº1), (nº2) e (nº3): "(1) Os capítulos 3 a 7 não se aplicam às informações pessoais indicadas em nenhum dos seguintes subparágrafos: 1. Informações pessoais coletadas pela Lei de Estatística entre informações pessoais processadas pelas instituições públicas;

			2. Informações pessoais coletadas ou com o fornecimento solicitado a fim de analisar as informações relacionadas à segurança nacional; 3. Informações pessoais processadas temporariamente, caso sejam urgentemente necessárias para a segurança e bem-estar públicos, saúde pública, etc .; ou 4. Informações pessoais coletadas e usadas para seus próprios fins de comunicação pela imprensa, atividades missionárias por organizações religiosas e nomeação de candidatos por partidos políticos, respectivamente. (2) Os Artigos 15, 22, 27 (1) e (2), 34 e 37 não se aplicam às informações pessoais processadas por meio de dispositivos visuais de processamento de dados instalados e operados em locais abertos, nos termos de cada subparágrafo do Artigo 25 (1). (3) Os artigos 15, 30 e 31 não se aplicam às informações pessoais processadas por um controlador de informações pessoais para operar grupos ou associações de amizade, como associações de ex-alunos e clubes de hobby.";

Somente a PIPA apresenta um rol de hipóteses no qual os princípios de proteção de informações pessoais e direitos de titulares de dados não se aplicam. A previsão está no artigo 58 (nº 1 a 3), com destaque para as informações pessoais: (i) coletadas em função da Lei de Estatística; (ii)

relacionadas à segurança nacional; (iii) processadas temporariamente e urgentemente para a segurança, bem-estar e saúde públicos; (iv) coletadas e usadas para fins de comunicação pela imprensa, atividade missionária por organizações religiosas e nomeação de candidatos por partidos políticos.

- **Quanto à relação jurídica entre sujeitos**

2.3. Transferência Internacional de Dados ou Processamento Transfronteiriço

De antemão, um quadro geral acerca da transferência internacional de dados no âmbito da APPI e da PIPA pode ser desenhado.

Primeiramente, com relação ao Japão, nota-se que as instruções sobre a matéria se encontram principalmente no art. 24 (nº1). Em regra, o controlador deve obter previamente o consentimento do titular para fornecer informações pessoais a um terceiro em país estrangeiro. As exceções dizem respeito ao país que celebre decisão de adequação ou ao terceiro que estabeleça um sistema de proteção de dados em conformidade com os padrões prescritos pela Comissão de Proteção.

Em segundo lugar, com relação à Coreia do Sul, a transferência internacional de dados está especificada no art. 17 (nº3), o qual prevê como única hipótese para tal o consentimento oferecido pelo titular. Ainda assim, a emenda nº 16.930 entrou em vigor no país, no dia 05 de agosto de 2020, com o intuito de aproximar a PIPA dos parâmetros do RGPD e obter decisão de adequação por parte da Comissão Europeia (KWANG HYUN RYOO, 2020).

2.3.1. Decisão de Adequação

Instituição Jurídica	Subtipo de Instituição Jurídica	APPI (Japão)	PIPA (Coreia do Sul)
Transferência Internacional de Dados ou Processamento Transfronteiriço	Decisão de Adequação	Artigo 24 (nº1): "(1) Um PIHBO (...) deverá, no caso de fornecer dados pessoais a um terceiro (...) em um país estrangeiro (significando um país ou	Não há previsão legal

		região localizado fora do território do Japão; a seguir, o mesmo) (**excluindo-se aqueles prescritos pelas regras da Comissão de Proteção de Informações Pessoais como um país estrangeiro que estabeleça um sistema de proteção de informações pessoais reconhecido como tendo um padrão equivalente ao do Japão em relação à proteção dos direitos e interesses de um indivíduo; a seguir, o mesmo neste Artigo, no parágrafo seguinte e no Artigo 26-2, parágrafo (1), item (ii)**), obter previamente o consentimento do titular no sentido de que ele ou ela aprove o fornecimento a um terceiro em país estrangeiro. Nesse caso, o previsto no Artigo anterior não se aplica"	

A APPI acolhe a celebração de decisões de adequação, pois, conforme destacado acima no art. 24 (nº1), um controlador está autorizado a fornecer dados pessoais a um terceiro no estrangeiro sem o consentimento do titular, caso o país respectivo adote um sistema de proteção com padrão equivalente ao do Japão.

2.3.2. Consentimento

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**APPI (Japão)**	**PIPA (Coreia do Sul)**
Transferência Internacional de Dados ou Processamento Transfronteiriço	Consentimento	Artigo 24 (nº1): "(1) Um PIHBO, com exceção daqueles casos previstos em cada item do artigo anterior, parágrafo (1), deverá, no caso de fornecer dados pessoais a um terceiro (...) em um país estrangeiro (significando um	Artigo 17 (nº3): "(3) O controlador de informações pessoais deve informar o titular dos dados sobre as questões previstas no parágrafo (2) e obter o consentimento do titular dos dados para fornecer dados

		país ou região localizado fora do território do Japão; a seguir, o mesmo) (...), **obter previamente o consentimento do titular no sentido de que ele ou ela aprove o fornecimento a um terceiro em país estrangeiro.** Nesse caso, o previsto no Artigo anterior não se aplica"	pessoais a terceiros no estrangeiro; e não deve celebrar um contrato para a transferência transfronteiriça de informações pessoais em violação desta Lei.";

Segundo pode se verificar pelo art. 24 (nº1) da APPI e pelo art. 17 (nº3) da PIPA, em regra, o controlador de dados deve obter o consentimento do titular para realizar a transferência de informações pessoais a terceiros fora do país.

A última emenda à APPI acrescentou o art. 24 (nº2), o qual melhor qualificou como deve ser o consentimento obtido nos termos do art. 24 (nº1). Agora, antes de o titular fornecer seu consentimento, o PIHBO deve informá-lo sobre o sistema protetivo do país estrangeiro, as ações tomadas pelo terceiro para salvaguardar informações pessoais, além de outras informações que sirvam de referência.

Da mesma forma, o art. 17 (nº3) da PIPA prevê, além da obtenção do consentimento, que o controlador de informações pessoais deva informar ao titular dos dados sobre as questões previstas no parágrafo (nº2), quais sejam: (i) o destinatário das informações pessoais; (ii) a finalidade para a qual o destinatário das informações pessoais usa essas informações; (iii) os dados pessoais a serem fornecidos; (iv) o período durante o qual o destinatário retém e usa informações pessoais; (v) o fato de o titular dos dados ter o direito de negar o consentimento e as desvantagens, se houver, decorrentes da negação do consentimento.

2.3.3. Contrato

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**APPI (Japão)**	**PIPA (Coreia do Sul)**
Transferência Internacional de Dados ou	Contrato	Artigo 24 (nº1): "(1) Um PIHBO (...) deverá, no caso de fornecer dados pessoais a um terceiro	Não há previsão legal

Processamento Transfronteiriço		(**excluindo-se uma pessoa que estabeleça um sistema em conformidade aos padrões prescritos pelas regras da Comissão de Proteção de Informações Pessoais, conforme necessário para a tomada contínua de ações equivalentes àquelas que um PIHBO deve adotar em relação ao tratamento de dados pessoais, de acordo com as disposições desta Seção (referida como "ação equivalente" no parágrafo (3)); doravante o mesmo neste parágrafo, no parágrafo seguinte e no Artigo 26-2, parágrafo (1), item (ii)**) em um país estrangeiro (significando um país ou região localizado fora do território do Japão; a seguir, o mesmo) (...), obter previamente o consentimento do titular no sentido de que ele ou ela aprove o fornecimento a um terceiro em país estrangeiro. Nesse caso, o previsto no Artigo anterior não se aplica"	

Além de autorizar a transferência internacional de dados mediante o consentimento do titular ou a celebração de uma decisão de adequação, a APPI, em seu art. 24 (nº1), cita a hipótese em que o terceiro demonstra estabelecer um sistema de proteção de dados em conformidade com os padrões prescritos pela Comissão de Proteção de Informações Pessoais.

Nesse sentido, se compreende que a instituição desse sistema protetivo pode ser satisfeita, dentre outras vias, por meio de celebração contratual (HOUNSLOW e NOZAKI, 2020), ainda que a Lei não mencione o mecanismo diretamente.

A PIPA, por sua vez, não prevê a possiblidade de transferência de informações pessoais a outro país somente pelo oferecimento, por terceiro, de garantias de cumprimento de direitos e deveres, ainda que por contrato.

2.3.4. Regras Vinculativas Aplicáveis às Empresas

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**APPI (Japão)**	**PIPA (Coreia do Sul)**
Transferência Internacional de Dados ou Processamento Transfronteiriço	Regras Vinculativas Aplicáveis às Empresas	Artigo 24 (nº1): "(1) Um PIHBO (...) deverá, no caso de fornecer dados pessoais a um terceiro (**excluindo-se uma pessoa que estabeleça um sistema em conformidade aos padrões prescritos pelas regras da Comissão de Proteção de Informações Pessoais, conforme necessário para a tomada contínua de ações equivalentes àquelas que um PIHBO deve adotar em relação ao tratamento de dados pessoais, de acordo com as disposições desta Seção (referida como "ação equivalente" no parágrafo (3)); doravante o mesmo neste parágrafo, no parágrafo seguinte e no Artigo 26-2, parágrafo (1), item (ii)**) em um país estrangeiro (significando um país ou região localizado fora do território do Japão; a seguir, o mesmo) (...), obter previamente o consentimento do titular no sentido de que ele ou ela aprove o fornecimento a um terceiro em país estrangeiro. Nesse caso, o previsto no Artigo anterior não se aplica"	Não há previsão legal

O trecho em destaque no art. 24 (nº1) da APPI autoriza a transferência de dados a pessoa, fora do território japonês, que estabeleça um sistema de tratamento em conformidade com o padrão prescrito pela Comissão de Proteção.

Nesse sentido, de maneira semelhante ao tópico anterior 2.3.3, se compreende que a adequação às exigências da Comissão pode acontecer, ainda que não exista menção direta ao mecanismo na APPI, mediante a adoção, pelo terceiro no estrangeiro, de normas corporativas globais (em inglês, *Binding Corporate Rules*) (HOUNSLOW e NOZAKI, 2020).

Essas normas corporativas seriam a política interna de proteção de dados das empresas de um grupo econômico, compreendendo os princípios, direitos dos titulares e procedimentos internos relacionados ao tema (LEONARDI, 2021, p. 305).

Por fim, observa-se que a hipótese de estabelecimento de regras vinculativas aplicáveis às empresas somente pode ser suscitada no âmbito japonês.

2.3.5. Certificados e Códigos de Conduta

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**APPI (Japão)**	**PIPA (Coreia do Sul)**
Transferência Internacional de Dados ou Processamento Transfronteiriço	Certificados e Códigos de Conduta	Artigo 24 (nº1): "(1) Um PIHBO (...) deverá, no caso de fornecer dados pessoais a um terceiro (**excluindo-se uma pessoa que estabeleça um sistema em conformidade aos padrões prescritos pelas regras da Comissão de Proteção de Informações Pessoais, conforme necessário para a tomada contínua de ações equivalentes àquelas que um PIHBO deve adotar em relação ao tratamento de dados pessoais, de acordo com as disposições desta Seção (referida como "ação equivalente" no parágrafo**	Não há previsão legal

		(3)); doravante o mesmo neste parágrafo, no parágrafo seguinte e no Artigo 26-2, parágrafo (1), item (ii)) em um país estrangeiro (significando um país ou região localizado fora do território do Japão; a seguir, o mesmo) (...), obter previamente o consentimento do titular no sentido de que ele ou ela aprove o fornecimento a um terceiro em país estrangeiro. Nesse caso, o previsto no Artigo anterior não se aplica"	

Novamente, seguindo o mesmo raciocínio do tópico 2.3.4 acima, compreende-se que, com base no art. 24 (nº1) da APPI, o ordenamento japonês autoriza a transferência internacional de dados a terceiro que apresente certificados e códigos de conduta. Ou seja, uma pessoa pode comprovar o estabelecimento de um sistema em conformidade com os padrões prescritos pela Comissão de Proteção mediante alguma acreditação ou certificação (ISHIARA, 2020, p. 275).

Em relação à Coreia do Sul, reitera-se que a hipótese não se aplica, tendo em vista que a PIPA aprova somente o consentimento do titular como fundamento para transferências internacionais de dados.

3. Conclusões acerca das principais divergências e convergências entre a APPI e PIPA

Depois da análise das variáveis jurídicas realizada acima, pode se concluir que maiores são as semelhanças entre a APPI e a PIPA do que as diferenças, de forma que o nível de proteção de dados pessoais oferecido por ambas é similar.

Em suma, quanto à autoridade de proteção de dados, tanto o Japão quanto a Coreia do Sul constituíram órgão de controle independente para o desempenho de suas funções. Essa característica é essencial para a efetiva salvaguarda de dados pessoais.

Quanto aos direitos dos titulares, o primeiro destaque se dá em relação à adoção, nos dois países, de um conceito expansionista de quem sejam esses indivíduos, ampliando-se o número daqueles que são abarcados pelas respectivas leis.

Além disso, tanto no Japão quanto na Coreia do Sul são garantidos aos titulares de dados os direitos de ser informado, de acesso, de retificação, de revogação, de limitação do tratamento e de bloqueio ou restrição do processamento. É certo que os direitos de revogação, de limitação do tratamento e de bloqueio ou restrição do processamento são mais amplamente assegurados na Coreia do Sul, mas sem prejuízo do exercício desses por titulares sob a jurisdição da lei japonesa.

Ademais, o direito à intervenção humana na tomada de decisão e criação de perfil automatizadas, à portabilidade de dados e ao esquecimento não estão previstos nem pela APPI, nem pela PIPA, de forma que nenhuma oferece garantia maior ou menor do que a outra quanto a esses dois quesitos.

Ainda em relação aos direitos dos titulares, as diferenças entre o Japão e a Coreia do Sul se dão quanto à presença, no âmbito coreano, do direito ao apagamento e de limitações aos direitos dos titulares em geral, mediante um rol com hipóteses de exceção à ampla aplicação de direitos e princípios de proteção de dados pessoais.

No que diz respeito à transferência internacional de dados, ambos os países apresentam como regra geral a obtenção do consentimento do titular para isso, sendo esta a forma mais fundamental e básica de se exercer o controle sobre esse tipo de processamento.

A legislação do Japão, no entanto, vai além, prevendo como exceções ao consentimento decisão de adequação firmada com outro país ou o estabelecimento, por terceiro, de sistema conforme os padrões da Comissão de Proteção, o que, a princípio, poderia ser feito por contrato, normas corporativas globais ou certificados.

Em suma, a APPI acomoda todas as hipóteses mencionadas no presente estudo como fundamento para se transferir dados a terceiro no estrangeiro, enquanto a PIPA admite o consentimento somente.

CAPÍTULO 3: Aspectos convergentes e divergentes entre a Lei sobre a Proteção de Informações Pessoais do Brasil, do Japão e da Coreia do Sul

1. Questões preliminares

Esse capítulo se dedicará a cotejar a LGPD em relação à APPI (Japão) e à PIPA (Coreia do Sul), sob a ótica do Modelo TLICS, com o intuito de compreender se as leis japonesa e coreana oferecem proteção de dados em grau semelhante à brasileira.

Importa reiterar que a comparação abarcará apenas 18 das 51 variáveis jurídicas presentes no Modelo TLICS, as quais se organizam em 3 categorias: autoridade de proteção de dados, direitos individuais dos titulares e hipóteses de transferência internacional de dados. Conforme se afirmou no Capítulo 2, essa escolha tem a finalidade de permitir a apresentação das variáveis mais representativas em formato passível de compreensão quando da comparação de três leis diferentes.

2. Aspectos convergentes e divergentes entre a LGPD e a APPI

- **Quanto à entidade jurídica**

2.1. Autoridade de proteção de dados

A instituição de uma autoridade supervisora de marcos regulatórios em proteção de dados é essencial para a matéria, tanto por conta da dificuldade de o próprio titular acompanhar a efetividade de seus direitos de dados, quanto em função das frequentes mudanças tecnológicas envolvidas nesse campo (DONEDA, 2021, p. 467).

É o que se compreende desde as primeiras leis da disciplina, com destaque para a Carta de Direitos Fundamentais da União Europeia de 2000, segundo a qual autoridades de garantias seriam necessárias para a concretização do direito fundamental à proteção de dados pessoais (DONEDA, 2021, p. 467).

Uma autoridade de garantia, portanto, é constituída para resguardar direitos, a exemplo, no Brasil, da Autoridade Nacional de Proteção de Dados (ANPD) (DONEDA, 2021, p. 469-470) e, no Japão, da Comissão de Proteção de Informações Pessoais.

Mais precisamente em relação à ANPD, tem-se que é competente para zelar pela proteção de dados, elaborar diretrizes para uma política nacional nesse âmbito, fiscalizar e aplicar sanções em casos de tratamentos que descumpram a lei, promover a educação da população na matéria, dentre outras funções (art. 55-J, I, III, IV e VI). Sua modelagem institucional, por sua vez, está estabelecida no Decreto nº 10.474, de 26 de agosto de 2020, o qual entrará em vigor na data da publicação da nomeação do Diretor-Presidente da ANPD (art. 6º).

2.1.1. Autônoma/Independente

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**LGPD (Brasil)**	**APPI (Japão)**
Autoridade de Proteção de Dados	Autônoma/ Independente		Artigo 59 (nº2) e artigo 62: "(2) A Comissão pertence à jurisdição do Primeiro Ministro"; "O presidente e os comissários da Comissão devem exercer a sua autoridade oficial de forma independente".
	Não Autônoma/ Não Independente	Artigo 5º (XIX): "autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional"	

Uma das características fundamentais da autoridade de garantias que atuará na proteção de dados, sendo inclusive sua razão de existir, é a independência (DONEDA, 2021, p. 471). Para isso, é necessário afastar do

órgão a influência dos poderes estatais constituídos na administração pública direta (DONEDA, 2021, p. 471).

Alguns mecanismos podem ser implementados com o intuito de cumprir com esse objetivo, a exemplo (DONEDA, 2021, p. 471-473): (i) da limitação da discricionariedade na escolha dos seus membros, como a exigência de certa formação ou atuação profissional, além da presença de pessoal especializado em assuntos jurídicos, regulatórios e técnicos acerca de tratamento de dados; (ii) do estabelecimento de critérios como mandato fixo, a fim de que os dirigentes executem suas funções de forma autônoma e isonômica; (iii) do óbice à atuação dos membros simultaneamente a outras atividades, atuais ou até futuras, nesse último caso, pela estipulação de uma "quarentena" para diretores que se lançarão em novas ocupações; (iv) da concessão de poder de gerência sobre o próprio orçamento e estrutura; (v) da existência de autonomia técnica para proferir opiniões e decisões no âmbito de sua competência; (vi) da não subordinação hierárquica de suas atividades fiscalizatória, sancionatória e decisional, em relação a outros órgãos; (vii) da não vinculação hierárquica com o governo, com a consequente ausência de ingerência governamental sobre os atos da autoridade.

Com base nos requisitos elencados acima, pode-se concluir que a ANPD é, do ponto de vista formal, uma autoridade de proteção de dados independente, apresentando muitas daquelas características: (i) os membros do Conselho Diretor, seu órgão máximo de direção, devem ser escolhidos dentre brasileiros que tenham elevado conceito no campo de especialidade dos cargos para os quais serão nomeados (art. 55-C, § 2º da Lei nº 13.709/18), além de se exigir dos membros representativos da sociedade a comporem o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (daqui em diante, CNPDP) qualificação compatível com as matérias afetas à tarefa (art. 15, § 4º, I do Decreto nº 10.474/20); (ii) os membros do Conselho Diretor terão mandato de 4 (quatro) anos (art. 55-C, § 3º da Lei nº 13.709/18), somente perdendo seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar (art. 55-E da Lei nº 13.709/18); (iii) os cargos dos membros do Conselho Diretor são de dedicação exclusiva (art. 6º do Decreto nº 10.474/20), além de configurar conflito de interesses quando um dos membros, após o exercício do cargo, no período

de 6 (seis) meses, presta serviço a pessoa física ou jurídica com quem tenha estabelecido relacionamento relevante em razão do exercício da função ou estabelece vínculo profissional com pessoa física ou jurídica que desempenhe atividade relacionada à área de competência do antigo cargo (art. 55-F da Lei nº 13.709/18 c/c art. 6º da Lei nº 12.813); (iv) o Diretor-Presidente tem a prerrogativa de ordenar as despesas referentes à ANPD e de submeter a proposta orçamentária da entidade à aprovação do Conselho Diretor (art. 25 do Decreto nº 10.474/20); (v) garantia de autonomia técnica e decisória à ANPD (art. 55-B da Lei nº 13.709/18); (vi) no que se refere à proteção de dados pessoais, as competências da ANPD prevalecem sobre as de outras entidades ou órgãos da administração pública, além de deter competência exclusiva para aplicar as sanções previstas na LGPD e de ser o órgão central para interpretar a referida Lei e estabelecer normas e diretrizes para a sua implementação (art. 55-K da Lei nº 13.709/18).

No entanto, se reconhece no presente trabalho que a ANPD pode ter sua independência enfraquecida, do ponto de vista material, a depender de como se conduzirá sua relação com a administração direta.

Isso porque, além de a Autoridade Nacional ser órgão integrante da Presidência da República (art. 55-A da LGPD), a Casa Civil concentra grande poder em seu âmbito, na medida em que os conselheiros setoriais que formam o CNPDP são escolhidos por ato discricionário do Conselho Diretor, referendado pela Casa Civil, a partir do Decreto nº 10.474/20 (art. 15, §§ 5º e 6º) (DONEDA, 2021, p. 475).

Assim, diante da falta de mecanismos para que cada setor representado no CNPDP indique os nomes que julgarem mais adequados à função, há uma possibilidade de que conselheiros desalinhados às demandas do seu setor respectivo sejam eventualmente nomeados (DONEDA, 2021, p. 275). Nesse sentido, se enfraquece o modelo multissetorial do Conselho Nacional, o qual é desejável para a compreensão do ponto de vista de diferentes esferas da sociedade acerca da proteção de dados pessoais e consequente fortalecimento da independência da ANPD (DONEDA, 2021, p. 475).

Por fim, não se pode esquecer que a Autoridade Nacional tem natureza jurídica transitória e poderá ser transformada em entidade da administração

pública federal indireta em até 2 (dois) anos da data de entrada em vigor da sua estrutura regimental (art. 55-A, §§ 1º e 2º da Lei nº 13.709/18).

Quanto ao Japão, reitera-se que a Comissão de Proteção de Informações Pessoais exerce sua autoridade de forma independente.

2.1.2. Apresentação unitária

Instituição Jurídica	Subtipo de Instituição Jurídica	LGPD (Brasil)	APPI (Japão)
Autoridade de Proteção de Dados	Apresentação Unitária	Artigo 5º (XIX): "autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional"	Artigo 59 (nº2): "(2) A Comissão pertence à jurisdição do Primeiro-Ministro.";

Conforme o art. 5º, XIX, da LGPD, a autoridade nacional tem poder para fazer cumprir a referida lei em todo o território nacional.

Dessa forma, a ANPD, assim como a Comissão de Proteção de Informações Pessoais do Japão, tem organização unitária e, não, federativa.

- **Quanto à qualidade jurídica**

2.2. Titulares de Dados

2.2.1. Definição

Instituição Jurídica	Subtipo de Instituição Jurídica	LGPD (Brasil)	APPI (Japão)
Titulares de Dados	Definição	Artigo 5º (V): "titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento"	Artigo 2º (nº 8): "(8) Um 'titular' de informações pessoais, nesta Lei, significa um indivíduo específico identificável por informações pessoais"

A LGPD intitula o titular de dados apenas como “titular”, da mesma forma que a APPI. Segundo o art. 5º, V da lei brasileira, o termo designa “*pessoa natural a quem se referem os dados pessoais que são objeto de tratamento*”. Dado pessoal, por sua vez, é a informação pessoal relacionada a pessoa natural identificada ou identificável (art. 5º, I da LGPD).

Com essas duas informações, pode se concluir que o conceito de titular na LGPD e na APPI é bastante aproximado, tendo em vista que, em ambas as ocorrências, o titular é o ser humano cujos dados pessoais o fazem identificado ou identificável quando tratados.

Conforme se discutiu no tópico 2.2.1 do Capítulo 2, a presença do termo “identificável”, afora somente “identificado”, designa uma compreensão expansionista de quem sejam os indivíduos a serem resguardados pela LGPD e pela APPI. Em outras palavras, tanto a LGPD quanto a APPI ampliaram o escopo de quem deve ter seus dados tutelados.

2.2.2. Direito de ser informado

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**LGPD (Brasil)**	**APPI (Japão)**
Titulares de Dados	Direito de Ser Informado	Artigo 6º (VI): "transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial"	Artigo 27 (nº1; i a iv): "(1) Um PIHBO, em relação às informações pessoais retidas por si, disponibilizará os tópicos descritos a seguir de forma que o titular possa conhecê-los (incluindo aqueles casos em que, a pedido de um titular, responderá sem demora).

O direito de ser informado é guarnecido de forma ampla pela LGPD no art. 6º, VI, o qual garante aos titulares a obtenção de informações claras, precisas e facilmente acessíveis acerca do tratamento de seus dados e dos agentes que realizam esse processo.

No tópico 2.2.2 do Capítulo 2, se estabeleceu que a APPI, em seu art. 27 (nº1; ii), informa que o controlador disponibilizará, de maneira que o titular possa conhecer, a finalidade de utilização de seus dados pessoais retidos, dentre

outros tópicos. A mesma garantia é oferecida pela LGPD, tendo em vista que, além de o art. 6º, VI assegurar amplamente o princípio da transparência, o inciso I do mesmo artigo afirma que o tratamento de dados deve ser realizado conforme propósitos legítimos e informados ao titular.

Por fim, ainda quanto ao direito de ser informado, pode se falar que, no âmbito da LGPD, não é possível o compartilhamento de dados pessoais com terceiros de forma oculta (FLUMIGNAN e FLUMIGNAN, 2020, p. 132). O mesmo é segurado na APPI, segundo a qual o controlador, com algumas exceções, não fornecerá dados pessoais a terceiros sem obter o consentimento prévio do titular (art. 23, nº1).

2.2.3. Direito de Acesso

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**LGPD (Brasil)**	**APPI (Japão)**
Titulares de Dados	Direito de Acesso	Artigo 6º (IV): "livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais"	Artigo 28 (nº1): "(1) Um titular pode exigir de um PIHBO a divulgação de dados pessoais retidos que possam identificar ele ou ela por um método de fornecimento de registro eletromagnético ou outros métodos prescritos pelas regras da Comissão de Proteção de Informações Pessoais."

A APPI assegura ao titular a possiblidade de exigir do controlador a divulgação de seus próprios dados pessoais retidos (art. 28, nº1).

No mesmo sentido, a LGPD reconhece o direito subjetivo do titular de acesso às suas informações, de modo que possa consultar a integralidade delas facilitada e gratuitamente (art. 6º, IV). O diferencial desse artigo, em relação à lei japonesa, diz respeito à ampliação do direito de acesso ao garantir, também, a consulta da forma e da duração do tratamento de determinado dado pessoal.

2.2.4. Direito à Retificação

Instituição Jurídica	Subtipo de Instituição Jurídica	LGPD (Brasil)	APPI (Japão)
Titulares de Dados	Direito à Retificação	Artigo 18 (III): "correção de dados incompletos, inexatos ou desatualizados"	Artigo 29 (nº1): "(1) Um titular pode, quando o conteúdo de dados pessoais retidos que podem identificá-lo não estiver exato, exigir que um PIHBO faça uma correção, adição ou exclusão (de agora em diante denominada "correção etc." no presente artigo) em relação ao conteúdo dos dados pessoais retidos."

A LGPD, no seu art. 18, III, estatui que o titular tem o direito de obter do controlador a correção de seus dados que estejam incompletos, inexatos ou desatualizados. Essa previsão realiza o princípio da qualidade dos dados, segundo o qual, ao titular, são garantidas a exatidão, a clareza, a relevância e a atualização de suas informações pessoais (art. 6º, V da LGPD) (LIMA e RAMIRO, 2020, p. 258).

Da mesma forma, a APPI confere instrumentos para que o titular promova a correção, adição ou exclusão do conteúdo de dados inexatos (art. 29, nº1).

2.2.5. Direito ao Esquecimento ou Direito ao Apagamento

Instituição Jurídica	Subtipo de Instituição Jurídica	LGPD (Brasil)	APPI (Japão)
Titulares de Dados	Direito ao Esquecimento ou Direito ao Apagamento	Não há previsão legal	Não há previsão legal

Na LGPD, não há menção ao direito ao esquecimento ou apagamento. No máximo, pode se falar em uma aproximação da noção de direito ao apagamento, presente na lei europeia, com o direito à eliminação, previsto no art. 18, VI da lei brasileira. Segundo esse artigo "*O titular dos dados pessoais*

tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei".

Quanto à realização do direito ao esquecimento propriamente, a LGPD se distancia ainda mais desse objetivo. Sendo o direito ao esquecimento autônomo, conforme a diferenciação doutrinária apresentada no tópico 2.2.5 do Capítulo 2, não se identificou acolhimento deste por parte da LGPD.

Do mesmo modo, a APPI não garante o direito ao apagamento ou ao esquecimento.

2.2.6. Direito à Revogação

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**LGPD (Brasil)**	**APPI (Japão)**
Titulares de Dados	Direito à Revogação	Artigo 18 (IX): "revogação do consentimento, nos termos do § 5º do art. 8º desta Lei"	Artigo 30 (nº1) e (nº5): "(1) Um titular pode, quando dados pessoais retidos que possam identificá-lo estão sendo tratados em violação às disposições do Artigo 16 ou Artigo 16-2, ou, foram adquiridos em violação às disposições do Artigo 17, exigir de um PIHBO a cessação da utilização ou eliminação (doravante referida como "cessação da utilização etc." neste Artigo) dos dados pessoais retidos."; "(5) Um titular pode exigir que o PIHBO cumpra uma cessação de utilização etc. dos dados pessoais retidos, ou cesse uma provisão a terceiros, se tiver se tornado desnecessário para o PIHBO utilizar dados pessoais retidos que possam identificar o titular, se uma situação prescrita na cláusula principal do Artigo 22-2, parágrafo (1) ocorreu em conexão com os

			dados pessoais retidos que possam identificar o titular, ou existe a possibilidade de que o tratamento dos dados pessoais retidos que possam identificar o titular prejudiquem os direitos ou interesses legítimos desse."

O direito à revogação pode ser exercido pelos titulares tanto na esfera da LGPD quanto da APPI, sendo mais amplamente garantido, porém, pela lei brasileira, conforme se verificará.

No âmbito da APPI, o art. 30 (nºs 1 e 5) permite aos titulares o exercício da revogação através da exigência de que o controlador elimine dados que sejam: empregados em finalidade diferente da originária; adquiridos ou utilizados impropriamente; desnecessários ao controlador; acidentalmente vazados ou prejudiciais aos interesses legítimos do titular, caso tratados.

Já no escopo da LGPD, o direito à revogação é garantido aos titulares no art. 18, IX, sem outras delimitações restritivas (MARCACINI, 2020, p. 158). Se observa que a revogação do titular somente põe fim ao tratamento quando o consentimento primeiramente o autorizou, de forma que, nos casos em que o processamento independe da vontade ou interesse do titular, não cabe a esse vetá-lo, ao menos enquanto perdurar a autorização legal (MARCACINI, 2020, p. 158).

2.2.7. Direito à Limitação do Tratamento

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**LGPD (Brasil)**	**APPI (Japão)**
Titulares de Dados	Direito à Limitação do Tratamento	Artigo 18 (IV): "anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei"	Artigo 16 (nº1), Artigo 29 (nº1) e Artigo 30 (nº1) e (nº5): "(1) Um PIHBO não deve tratar informações pessoais, sem obter previamente o consentimento do titular, para além do âmbito necessário para cumprir uma finalidade de utilização especificada de

			acordo com o disposto no artigo anterior."; "(1) Um titular pode, quando o conteúdo de dados pessoais retidos que podem identificá-lo não estiver exato, exigir que um PIHBO faça uma correção, adição ou exclusão (de agora em diante denominada "correção etc." no presente artigo) em relação ao conteúdo dos dados pessoais retidos."; "(1) Um titular pode, quando dados pessoais retidos que possam identificá-lo estão sendo tratados em violação às disposições do Artigo 16 ou Artigo 16-2, ou, foram adquiridos em violação às disposições do Artigo 17, exigir de um PIHBO a cessação da utilização ou eliminação (doravante referida como “cessação da utilização etc.” neste Artigo) dos dados pessoais retidos."; "(5) Um titular pode exigir que o PIHBO cumpra uma cessação de utilização etc. dos dados pessoais retidos, ou cesse uma provisão a terceiros, se tiver se tornado desnecessário para o PIHBO utilizar dados pessoais retidos que possam identificar o titular, se uma situação prescrita na cláusula principal do Artigo 22-2, parágrafo (1) ocorreu em conexão com os dados pessoais retidos que possam identificar o titular, ou existe a possibilidade de que o tratamento dos dados pessoais retidos que possam identificar o titular prejudiquem os direitos ou interesses legítimos desse."

O direito à limitação do tratamento de dados é salvaguardado tanto pela LGPD, quanto pela APPI.

No caso da legislação brasileira, segundo o art. 18, IV da LGPD, dados considerados desnecessários ou excessivos ao cumprimento da finalidade do tratamento ou, ainda, tratados sem conformidade com o que demanda a Lei, devem ser anonimizados, bloqueados ou eliminados.

Em suma, o direito à limitação do tratamento de dados, por meio do bloqueio ou eliminação desses, ocorre em duas hipóteses: quando o tratamento é licito, mas os dados são desnecessários ou excessivos; ou, quando o tratamento for ilícito (LIMA e RAMIRO, 2020, p. 259).

A primeira hipótese visa cumprir os princípios da finalidade, adequação e necessidade (art. 6º, I, II e III da LGPD) (LIMA e RAMIRO, 2020, p. 259). Cabe apontar que, se os dados forem desnecessários ou excessivos, descumprirão os comandos dos princípios citados e, consequentemente, o tratamento não obedecerá à lei (LIMA e RAMIRO, 2020, p. 259). No entanto, a regra da segunda hipótese é mais abrangente e leva em consideração qualquer outra razão pela qual o tratamento seja ilícito (LIMA e RAMIRO, 2020, p. 259).

A legislação japonesa, por sua vez, conforme o art. 16 (nº1) da APPI, limita o tratamento dos dados de seus titulares quando orienta que um controlador não deve tratar essas informações para além do escopo necessário para cumprir a finalidade de utilização especificada e explicitada, a não ser que obtenha o consentimento prévio do titular. Essa diretriz se aproxima do art. 18, IV da LGPD, que acaba por desencorajar o tratamento de dados desnecessários ou excessivos para a realização da finalidade de utilização ou de tratamento.

Destaca-se também o disposto ao final do art. 30 (nº5) da APPI, segundo o qual um titular pode exigir que o controlador cesse a utilização de seus dados pessoais, dentre outros casos, quando existe a possibilidade de que o tratamento prejudique seus direitos ou interesses legítimos. Similarmente, a LGPD afasta o tratamento prejudicial aos direitos ou interesses legítimos do titular quando oferece hipótese abrangente de limitação do tratamento ilícito de dados.

2.2.8. Direito de Portabilidade de Dados

Instituição Jurídica	Subtipo de Instituição Jurídica	LGPD (Brasil)	APPI (Japão)
Titulares de Dados	Direito de Portabilidade dos Dados	Artigo 18 (V): "portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial"	Não há previsão legal

Somente a LGPD assegura o direito à portabilidade de dados, consagrado no art. 18, V da norma.

Essa previsão foi inspirada no art. 20 do RGPD, segundo o qual o titular tem o direito de receber os dados que forneceu ao responsável por um tratamento, em formato estruturado, além do direito de fornecê-los a outro responsável por um tratamento (LIMA e RAMIRO, 2020, p. 271). O titular também teria o direito de que seus dados pessoais fossem transmitidos diretamente entre os responsáveis (LIMA e RAMIRO, 2020, p. 271).

Essa comparação serve para compreender melhor as garantias oferecidas pela LGPD. Nesse sentido, a norma brasileira também oferece o direito à portabilidade de dados a outro fornecedor de serviços ou produto mediante requisição expressa do titular. No entanto, não existe especificação do formato em que devem ser transmitidos e nem a possiblidade de transmissão direta entre agentes de tratamento (LIMA e RAMIRO, 2020, p. 271).

Conclui-se, assim, que tal regulamentação pela ANPD é muito relevante para a concretização do direito à portabilidade, pois, sem que o formato dos dados seja estruturado, a migração das informações para outro agente pode ser inviabilizada. Além disso, sem a possiblidade de portabilidade direita de dados entre agentes de tratamento, a migração também pode ser prejudicada, dada a pouca habilidade informacional que, em geral, o usuário tem (LIMA e RAMIRO, 2020, p. 271).

2.2.9. Direito a Bloqueio ou Restrição do Processamento

Instituição Jurídica	Subtipo de Instituição Jurídica	LGPD (Brasil)	APPI (Japão)
Titulares de Dados	Direito a Bloqueio ou Restrição do Processamento	Artigo 18 (IV): "anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei"	Artigo 29 (nº1) e Artigo 30 (nº1) e (nº5): "(1) Um titular pode, quando o conteúdo de dados pessoais retidos que podem identificá-lo não estiver exato, exigir que um PIHBO faça uma correção, adição ou exclusão (de agora em diante denominada "correção etc." no presente artigo) em relação ao conteúdo dos dados pessoais retidos."; "(1) Um titular pode, quando dados pessoais retidos que possam identificá-lo estão sendo tratados em violação às disposições do Artigo 16 ou Artigo 16-2, ou, foram adquiridos em violação às disposições do Artigo 17, exigir de um PIHBO a cessação da utilização ou eliminação (doravante referida como “cessação da utilização etc.” neste Artigo) dos dados pessoais retidos."; "(5) Um titular pode exigir que o PIHBO cumpra uma cessação de utilização etc. dos dados pessoais retidos, ou cesse uma provisão a terceiros, se tiver se tornado desnecessário para o PIHBO utilizar dados pessoais retidos que possam identificar o titular, se uma situação prescrita na cláusula principal do Artigo 22-2, parágrafo (1) ocorreu em conexão com os dados pessoais retidos que possam identificar o titular, ou existe a possibilidade de que o tratamento dos dados

			pessoais retidos que possam identificar o titular prejudiquem os direitos ou interesses legítimos desse."

O direito ao bloqueio ou à restrição de processamento está presente tanto na LGPD, quanto na APPI.

Conforme explicitado no tópico 2.6.6 do Capítulo 2, acerca desse direito na esfera da lei japonesa, o titular pode restringir ou bloquear o tratamento de seus dados ao demandar a correção ou a exclusão dessas informações, quando o seu conteúdo não estiver exato (art. 29 (nº1))**,** ou, ainda, ao pedir pela eliminação ou cessação de utilização de seus dados, em determinadas hipóteses (art. 30 (nº1 e nº5)).

Essas hipóteses delimitam, de certa forma, o exercício do direito ao bloqueio e à restrição do processamento por parte do titular. Os casos a que se refere o art. 30 (nºs 1 e 5) são os seguintes: o titular só pode exigir do controlador a eliminação e suspensão do tratamento de dados empregados em finalidade diferente da originária; adquiridos ou utilizados impropriamente; desnecessários ao controlador; acidentalmente vazados; e prejudiciais aos interesses legítimos do titular, caso tratados.

No direito brasileiro, tal garantia encontra guarida no art. 18, IV da LGPD, segundo o qual o titular tem o direito à anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto naquela lei. Assim, quando comparadas as normas dos dois países, observa-se que a redação do art. 18 da LGPD é ampla o suficiente para garantir proteção similar à APPI quanto ao bloqueio ou à restrição do processamento de dados.

2.2.10. Direito à Intervenção Humana na Tomada de Decisão e Criação de Perfil Automatizadas

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**LGPD (Brasil)**	**APPI (Japão)**
Titulares de Dados	Direito à Intervenção Humana na Tomada de	Artigo 20: "O titular dos dados tem direito a solicitar a revisão de	Não há previsão legal

	Decisão e Criação de Perfil Automatizadas	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"	

Em relação ao direito à intervenção humana na tomada de decisão e criação de perfil automatizadas, tem-se que apenas a LGPD se ocupa de mencioná-lo, ao prever instrumentos de controle mínimo quanto ao processamento automatizado de dados pessoais por empresas da economia digital, visando garantir algum grau de transparência e responsabilidade por parte delas (ANJOS, 2019).

O direito à revisão das decisões automatizadas garante que os titulares possam se opor a erros e práticas discriminatórias em casos em que há preconceito implícito ou resultado tendencioso por parte de algum algoritmo (SOUSA, PERRONE e MAGRANI, 2021, p. 277).

Assim, segundo o art. 20 da LGPD, o titular dos dados tem o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado e que afetem seus interesses, como as que definem seu perfil pessoal, profissional, de consumo, de crédito ou aspectos de sua personalidade.

Observa-se que o rol de hipóteses que autorizam a revisão de decisões automatizadas é satisfatoriamente amplo, por incluir também aquelas decisões destinadas a definir um aspecto da personalidade de um indivíduo (SOUSA, PERRONE e MAGRANI, 2021, p. 277). Ainda assim, é necessário pontuar que o escopo seria ainda mais amplo se incluísse decisões semiautomatizadas (SOUSA, PERRONE e MAGRANI, 2021, p. 277).

Além disso, com o veto presidencial ao § 3º do art. 20 da LGPD, não há mais referência explícita à intervenção humana nessa revisão, o que não é ideal (SOUSA, PERRONE e MAGRANI, 2021, p. 277). O critério não foi mantido sob o arrazoado de que a exigência da participação humana inviabilizaria o modelo de negócio de muitas empresas, contrariando o interesse público (PALHARES, 2019).

Como consequência, existe a possibilidade de a revisão da decisão de um algoritmo ser realizada por outro, tendo em vista que a redação atual do art. 20 não exige a intervenção de uma pessoa natural, ainda que essa seja a prática aconselhável para a efetivação do direito à revisão (SOUSA, PERRONE e MAGRANI, 2021, p. 277-278). A ideia é que se possibilite chegar a conclusões diversas das apresentadas pela primeira decisão, automatizada (SOUSA, PERRONE e MAGRANI, 2021, p. 278).

Ainda assim, é possível se falar em direito à intervenção humana na tomada de decisão e criação de perfil automatizadas no âmbito brasileiro, tendo em vista que não há indícios de que o texto impeça o estabelecimento da revisão mediante intervenção humana como padrão, levando-se em consideração que o propósito geral de transparência da LGPD em relação ao titular estaria mais bem efetivado assim (SOUSA, PERRONE e MAGRANI, 2021, p. 278).

Do mesmo modo, espera-se que a ANPD faça recomendações sobre o tema, indicando o grau de participação humana na revisão de decisões automatizadas (SOUSA, PERRONE e MAGRANI, 2021, p. 278).

2.2.11. Limitações

Instituição Jurídica	Subtipo de Instituição Jurídica	LGPD (Brasil)	APPI (Japão)
Titulares de Dados	Limitações	Não há previsão legal	Não há previsão legal

Tanto no âmbito da LGPD, quanto no da APPI, não existe um rol que elenque limites ao usufruto do direito de proteção de dados pessoais pelos titulares.

- **Quanto à relação jurídica entre sujeitos**

2.3. Transferência Internacional de Dados ou Processamento Transfronteiriço

O artigo 5º, inciso XV da LGPD configura transferência internacional de dados como sendo a transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o Brasil seja membro.

A legislação brasileira foi bastante influenciada pela europeia nesse setor, podendo-se citar, mais precisamente, as contribuições da Diretiva 95/46/CE e do Regulamento Geral Europeu sobre a Proteção de Dados Pessoais (LIMA e PEROLI, 2020, p. 72).

Com o advento da Diretiva 95/46/CE, passou a ser necessário comprovar, perante a Comissão da União Europeia, que o país para o qual os dados de europeus fossem encaminhados oferecia um nível adequado de proteção (LIMA e PEROLI, 2020, p. 70 e 71). Quando o Regulamento Geral sobre a Proteção de Dados (RGPD) entra em vigor no dia 25 de maio de 2018, se mantém a ideia de que a adequação ao padrão europeu de proteção de dados deva ser reconhecida, segundo avaliação da Comissão Europeia, para transferências internacionais de dados (LIMA e PEROLI, 2020, p. 71).

Depois desse sucinto panorama do entendimento europeu sobre transferências internacionais, volta-se novamente para a regulação da matéria no âmbito do Japão, segundo o art. 24 (nº1) da APPI, e do Brasil, segundo o art. 33 da LGPD.

No direito japonês, em regra, o controlador deve obter, previamente, o consentimento do titular para fornecer informações pessoais a um terceiro em país estrangeiro. As exceções dizem respeito a dois cenários: (i) à celebração de decisão de adequação entre os respectivos países; (ii) ou à adoção, pelo terceiro, de um sistema protetivo conforme os padrões da Comissão de Proteção de Informações Pessoais, que, a princípio, poderia ser implementado por meio de contratos, normas corporativas globais ou certificados.

No Brasil, todas essas possibilidades estão presentes, conforme se verá nos tópicos seguintes, sendo o consentimento, da mesma forma, a regra geral para autorizar uma transferência internacional de dados.

2.3.1. Decisão de Adequação

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**LGPD (Brasil)**	**APPI (Japão)**
Transferência Internacional de Dados ou Processamento Transfronteiriço	Decisão de Adequação	Artigo 33 (I): "para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais	Artigo 24 (nº1): "(1) Um PIHBO (...) deverá, no caso de fornecer dados pessoais a um terceiro (...) em um país estrangeiro

		adequado ao previsto nesta Lei"	(significando um país ou região localizado fora do território do Japão; a seguir, o mesmo) (**excluindo-se aqueles prescritos pelas regras da Comissão de Proteção de Informações Pessoais como um país estrangeiro que estabeleça um sistema de proteção de informações pessoais reconhecido como tendo um padrão equivalente ao do Japão em relação à proteção dos direitos e interesses de um indivíduo; a seguir, o mesmo neste Artigo, no parágrafo seguinte e no Artigo 26-2, parágrafo (1), item (ii)**), obter previamente o consentimento do titular no sentido de que ele ou ela aprove o fornecimento a um terceiro em país estrangeiro. Nesse caso, o previsto no Artigo anterior não se aplica"

Conforme a redação do art. 33, I da LGPD, em um contexto de transferências internacionais de dados, é necessário que o país ou organismo internacional considerado proporcione grau de proteção equivalente, ou adequado, ao exigido pelo Brasil.

A LGPD, no entanto, não elenca os critérios para que certo ordenamento seja considerado adequado, deixando essa incumbência a cargo da ANPD (CARVALHO, 2019, p. 625).

Assim, conforme o art. 34, *caput* da Lei, o nível protetivo do país ou organismo em questão será avaliado pela Autoridade Nacional, a qual levará em consideração as normas gerais e setoriais da legislação em vigor no local de destino, a natureza dos dados, a observância dos princípios gerais de proteção de dados pessoais e dos direitos dos titulares presentes na LGDP, a adoção de medidas de segurança, a existência de garantias judiciais e institucionais de respeito aos direitos de proteção de dados pessoais, dentre outros critérios.

Desse modo, a decisão da ANPD pode ser vista como uma declaração de idoneidade acerca de outro sistema normativo, por certo período, com efeitos amplos e gerais (CARVALHO, 2019, p. 626-627).

Justamente por isso, é fundamental que uma ANPD independente seja organizada com celeridade no Brasil, permitindo que empresas e agentes de tratamento transfiram dados para o país sem recorrer a outros meios de alto custo, viabilizando, além disso, que atores econômicos nacionais atuem a nível global (BIONI, FAVARO e RIELLI, 2020).

Quanto ao Japão, semelhantemente ao que se verifica no Brasil, o controlador pode, caso haja decisão de adequação, fornecer dados pessoais a um terceiro no estrangeiro sem o consentimento do titular, conforme o que se extrai do destaque no art. 24 (nº1) da APPI, na tabela acima.

2.3.2. Consentimento

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**LGPD (Brasil)**	**APPI (Japão)**
Transferência Internacional de Dados ou Processamento Transfronteiriço	Consentimento	Artigo 33 (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"	Artigo 24 (nº1): "(1) Um PIHBO, com exceção daqueles casos previstos em cada item do artigo anterior, parágrafo (1), deverá, no caso de fornecer dados pessoais a um terceiro (...) em um país estrangeiro (significando um país ou região localizado fora do território do Japão; a seguir, o mesmo), **obter previamente o consentimento do titular no sentido de que ele ou ela aprove o fornecimento a um terceiro em país estrangeiro**. Nesse caso, o previsto no Artigo anterior não se aplica"

Além da possibilidade de se conceber uma decisão de adequação, a LGPD prevê outros fundamentos pelos quais as transferências internacionais de dados possam acontecer. Isso inclui os casos elencados nos incisos III a VIII do

art. 33, hipóteses residuais que suscitam o afastamento do diploma por dizerem respeito a situações em que, ou a autoridade de proteção dados não certificou o nível de proteção propiciado por outro ordenamento, ou não há instrumentos para a defesa adequada de direitos fundamentais (CARVALHO, 2019, p. 629-630). Isso não significa, no entanto, uma derrogação completa da LGPD, pois sempre se observará o respeito aos direitos fundamentais, a exemplo da transferência internacional autorizada por consentimento específico (art. 33, VIII) (CARVALHO, 2019, p. 630-631).

Essa categoria autorizativa, inclusive, é uma hipótese legal válida não somente segundo a LGPD (art. 33, VIII), mas também conforme a APPI (art. 24 nº1).

No caso da lei brasileira, é necessário que o titular, ao fornecer o consentimento, esteja previamente informado do caráter internacional da transferência. No caso da lei japonesa, conforme já explicitado no Capítulo 2, o art. 24 (nº2) especifica que, antes de o titular conceder seu consentimento, o controlador deve informá-lo sobre o sistema de proteção de informações pessoais do país estrangeiro, as ações tomadas pelo terceiro para a proteção de informações pessoais, além de outras informações que sirvam de referência.

2.3.3. Contrato

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**LGPD (Brasil)**	**APPI (Japão)**
Transferência Internacional de Dados ou Processamento Transfronteiriço	Contrato	Artigo 33 (II, alíneas a e b): "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"	Artigo 24 (nº1): "(1) Um PIHBO (...) deverá, no caso de fornecer dados pessoais a um terceiro (**excluindo-se uma pessoa que estabeleça um sistema em conformidade aos padrões prescritos pelas regras da Comissão de Proteção de Informações Pessoais, conforme necessário para a tomada contínua de ações equivalentes àquelas que um PIHBO deve adotar em relação ao tratamento de dados pessoais, de acordo**

			com as disposições desta Seção (referida como "ação equivalente" no parágrafo (3)); doravante o mesmo neste parágrafo, no parágrafo seguinte e no Artigo 26-2, parágrafo (1), item (ii)) em um país estrangeiro (significando um país ou região localizado fora do território do Japão; a seguir, o mesmo) (...), obter previamente o consentimento do titular no sentido de que ele ou ela aprove o fornecimento a um terceiro em país estrangeiro. Nesse caso, o previsto no Artigo anterior não se aplica"

No presente tópico, bem como nos dois seguintes, se analisará um outro regime de transferência internacional de dados apresentado pela LGPD, no art. 33, inciso II. Conforme esse excerto, é permitida a transferência segura de dados a ordenamento jurídico pouco protetivo, em decorrência das garantias apresentadas pela autonomia privada entre as partes, sancionada pela autoridade nacional, perante os padrões da LGPD ou de autoridades privadas independentes (CARVALHO, 2019, p. 629). Em suma, ainda que um sistema normativo terceiro não atenda todas as exigências da LGPD, um controlador específico pode fazê-lo (CARVALHO, 2019, p. 267).

Essas iniciativas privadas, no entanto, precisam oferecer cláusulas que assegurem o cumprimento de um nível adequado de proteção de dados (CARVALHO, 2019, p. 628). Nesse sentido, o art. 35 da LGPD estabelece que a definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas, normas corporativas globais ou selos, certificados e códigos de conduta, todos instrumentos previstos no art. 33, II, da Lei, serão realizadas pela autoridade nacional (CARVALHO, 2019, p. 628). Essa definição também pode, de acordo com os indicadores da autoridade nacional, ser elaborada pelo mercado, através de certificações que atestem a adesão a determinado padrão corporativo (CARVALHO, 2019, p. 628).

Feito esse panorama geral do art. 33, II da LGPD, destaca-se nesse tópico a presença dos incisos “a” e “b”, segundo os quais uma transferência internacional de dados pode ocorrer quando, na forma de cláusulas contratuais específicas ou padrão, o controlador comprova o respeito aos princípios da Lei, aos direitos do titular, além do oferecimento de proteção de dados a nível adequado.

Em relação ao Japão, é possível suscitar o acolhimento da mesma hipótese, tendo em vista que a instituição de um sistema protetivo, por terceiro, em conformidade com as regras da Comissão de Proteção poderia, a princípio, se realizar mediante contrato (HOUNSLOW e NOZAKI, 2020), ainda que a APPI não faça alusão a esse recurso específico de modo expresso.

2.3.4. Regras Vinculativas Aplicáveis às Empresas

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**LGPD (Brasil)**	**APPI (Japão)**
Transferência Internacional de Dados ou Processamento Transfronteiriço	Regras Vinculativas Aplicáveis às Empresas	Artigo 33 (II, c): "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: c) normas corporativas globais"	Artigo 24 (nº1): "(1) Um PIHBO (...) deverá, no caso de fornecer dados pessoais a um terceiro (**excluindo-se uma pessoa que estabeleça um sistema em conformidade aos padrões prescritos pelas regras da Comissão de Proteção de Informações Pessoais, conforme necessário para a tomada contínua de ações equivalentes àquelas que um PIHBO deve adotar em relação ao tratamento de dados pessoais, de acordo com as disposições desta Seção (referida como “ação equivalente” no parágrafo (3)); doravante o mesmo neste parágrafo, no parágrafo seguinte e no Artigo 26-2, parágrafo (1), item (ii)**) em um país estrangeiro (significando um país ou região localizado fora

			do território do Japão; a seguir, o mesmo) (...), obter previamente o consentimento do titular no sentido de que ele ou ela aprove o fornecimento a um terceiro em país estrangeiro. Nesse caso, o previsto no Artigo anterior não se aplica"

A LGPD não elenca maiores critérios para as normas corporativas globais (VERONESE, 2021, p. 718). No entanto, pode-se afirmar que sejam semelhantes às *Binding Corporate Rules* ou BCRs (em português, “regras vinculativas aplicáveis às empresas”), apresentadas no art. 47 do RGPD (LEONARDI, 2021, p. 305).

Essas regras vinculativas seriam, assim, a política interna de proteção de dados das empresas de um grupo econômico, abarcando princípios, direitos dos titulares e procedimentos internos relacionados ao tema (LEONARDI, 2021, p. 305). Quando a autoridade nacional competente indica que seu conteúdo é suficientemente protetivo, as transferências de dados internas ao grupo, mesmo as internacionais, estarão em conformidade com o RGPD, dispensando nova aquiescência do órgão (LEONARDI, 2021, p. 305).

A LGPD não se manifesta abertamente sobre esse procedimento, mas se espera que a ANPD cumpra papel semelhante de aprovação de normas corporativas globais (LEONARDI, 2021, p. 305). Essa expectativa está em consonância com o art. 33, II da Lei, segundo o qual, para que uma transferência internacional de dados seja permitida, é necessário que o controlador ofereça garantias do cumprimento do regime de proteção da LGPD, por meio de normas corporativas globais, dentre outras alternativas (LEONARDI, 2021, p. 305). O art. 36 reforça esse entendimento ao afirmar que alterações nas garantias apresentadas pelas normas coorporativas globais deverão ser comunicadas à ANPD (LEONARDI, 2021, p. 305).

No âmbito japonês, normas corporativas globais também poderiam ser adotadas por terceiro no estrangeiro como demonstração de adequação às regras da Comissão de Proteção e evidência da existência de sistema protetivo pertinente (HOUNSLOW e NOZAKI, 2020).

2.3.5. Certificados e Códigos de Conduta

Instituição Jurídica	Subtipo de Instituição Jurídica	LGPD (Brasil)	APPI (Japão)
Transferência Internacional de Dados ou Processamento Transfronteiriço	Certificados e Códigos de Conduta	Artigo 33 (II, d): "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: d) selos, certificados e códigos de conduta regularmente emitidos"	Artigo 24 (nº1): "(1) Um PIHBO (...) deverá, no caso de fornecer dados pessoais a um terceiro (**excluindo-se uma pessoa que estabeleça um sistema em conformidade aos padrões prescritos pelas regras da Comissão de Proteção de Informações Pessoais, conforme necessário para a tomada contínua de ações equivalentes àquelas que um PIHBO deve adotar em relação ao tratamento de dados pessoais, de acordo com as disposições desta Seção (referida como "ação equivalente" no parágrafo (3)); doravante o mesmo neste parágrafo, no parágrafo seguinte e no Artigo 26-2, parágrafo (1), item (ii)**) em um país estrangeiro (significando um país ou região localizado fora do território do Japão; a seguir, o mesmo) (...), obter previamente o consentimento do titular no sentido de que ele ou ela aprove o fornecimento a um terceiro em país estrangeiro. Nesse caso, o previsto no Artigo anterior não se aplica"

A LGPD também autoriza que transferências internacionais de dados pessoais ocorram quando o controlador apresentar selo, certificado ou código de

conduta reconhecido pela ANPD, comprovando efetivar o regime de proteção da Lei (LEONARDI, 2021, p. 305).

Quanto à APPI, do mesmo modo, a constatação da existência de sistema protetivo consoante às regras da Comissão de Proteção poderia incluir a emissão de acreditação ou certificação (ISHIARA, 2020, p. 275).

3. Conclusões acerca das principais divergências e convergências entre a LGPD e a APPI

Em primeiro lugar, quanto à autoridade de proteção de dados, tanto o Brasil, quanto o Japão dispõem de órgãos, ao menos formalmente, independentes. Observa-se apenas que, no caso brasileiro, o exercício efetivamente autônomo das atividades da ANPD depende da postura a ser adotada pela Presidência da República quanto à ingerência no órgão, tendo em vista a relação de subordinação entre os dois, e da Casa Civil, quanto ao pleno exercício das atividades do CNPDP.

Ademais, o Brasil e o Japão possuem autoridades que se apresentam de forma unitária, sendo elas, respectivamente, a Autoridade Nacional de Proteção de Dados (ANPD) e a Comissão de Proteção de Informações Pessoais (Comissão).

Em segundo lugar, no âmbito dos direitos dos titulares, tanto o Brasil quanto o Japão, por acatarem um conceito expansionista de quem seja o titular, ampliaram o número daqueles que são destinatários das garantias oferecidas por suas leis de proteção de dados.

Quanto aos direitos dos titulares, especificamente, apreendeu-se que ambos os sistemas normativos buscam provê-los amplamente. Assim, das 10 (dez) categorias relacionadas a direitos de titulares apresentadas entre os tópicos 2.2.2 e 2.2.11 do presente capítulo, em 6 (seis) delas, tanto o Brasil quanto o Japão ostentam previsão legal; em 2 (duas), nenhum dos dois países se manifesta; e, em 2 (duas), somente o Brasil prevê alguma garantia.

Mais precisamente quanto às coincidências, a LGPD e a APPI promovem adequadamente a seus titulares, ainda que, quanto a uma ou outra categoria, de forma mais ou menos ampla, o direito de: (i) ser informado; (ii) de acesso; (iii) à

retificação; (iv) à revogação; (v) à limitação do tratamento; e, (vi) ao bloqueio ou restrição do processamento.

Relativamente às categorias não mencionadas nem na LGPD, nem na APPI, estão o direito ao esquecimento ou ao apagamento, além de rol de limitações dos direitos do titular. Interessante observar que, na realidade, o Brasil e o Japão promovem maior fruição de direitos pelos titulares, uma vez que não trazem em seu diploma normativo alistamento de restrições para aplicação de suas garantias.

Ainda quanto aos direitos dos titulares, no que se refere às divergências entre a LGPD e a APPI, tem-se que somente o Brasil prevê o direito de portabilidade de dados e o direito à intervenção humana na tomada de decisão e criação de perfil automatizadas.

Em terceiro e último lugar, no tocante à transferência internacional de dados, todas as 5 (cinco) categorias de autorização elencadas entre os tópicos 2.3.1 e 2.3.5 desse capítulo se aplicam aos dois países. Deste modo, tanto no Brasil quanto no Japão, dados pessoais podem ser transferidos a terceiro no estrangeiro em função de decisão de adequação; do consentimento do titular; de celebração contratual; de adoção de normas corporativas globais; e, por fim, em decorrência da emissão de certificações.

Assim, por meio da análise realizada pela ótica do modelo TLICS nos tópicos 2.1, 2.2 e 2.3 desse capítulo, identificou-se inúmeras congruências entre o sistema normativo brasileiro e o japonês, no que diz respeito à existência de uma autoridade de proteção de dados independente, ao oferecimento de amplas garantias aos titulares e à regulamentação de transferências internacionais de dados. Conclui-se, desse modo, que há comensurabilidade entre a LGPD e a APPI, de forma que a transferência de dados pessoais entre o Japão e o Brasil é segura.

4. Aspectos convergentes e divergentes entre a LGPD e a PIPA

- **Quanto à entidade jurídica**

4.1. Autoridade de proteção de dados

No Brasil, conforme a LGPD, a Autoridade Nacional de Proteção de Dados (ANPD) é o órgão competente para zelar pela proteção dos dados dos titulares. Essa figura é exercida na Coreia do Sul, segundo a PIPA, pela Comissão de Proteção de Informações Pessoais (Comissão de Proteção).

4.1.1. Autônoma/Independente

Instituição Jurídica	Subtipo de Instituição Jurídica	LGPD (Brasil)	PIPA (Coreia do Sul)
Autoridade de Proteção de Dados	Autônoma/ Independente		Artigo 7º (nº1) e (nº2): "(1) A Comissão de Proteção de Informações Pessoais (doravante referida como a "Comissão de Proteção") será estabelecida pelo Primeiro-Ministro para conduzir de forma independente o trabalho relacionado com a proteção de informações pessoais. (2) A Comissão de Proteção será considerada uma agência administrativa central nos termos do Artigo 2 da Lei de Organização do Governo (...)"
	Não Autônoma/ Não Independente	Artigo 5º (XIX): "autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional"	

Em relação ao exercício de suas funções, tanto a Autoridade Nacional de Proteção de Dados, quanto a Comissão de Proteção de Informações Pessoais têm condições realiza-las de forma independente.

De acordo com o artigo 7º (nº1) da PIPA, a Comissão de Proteção conduz seus trabalhos independentemente, ainda que seja estabelecida pelo Primeiro Ministro.

A ANPD, por sua vez, apesar de ser órgão subordinado à Presidência da República, reúne outras características que conferem a ela, do ponto de vista formal, independência funcional, conforme demonstrado no tópico 2.1.1 desse capítulo.

4.1.2. Apresentação Unitária

Instituição Jurídica	Subtipo de Instituição Jurídica	LGPD (Brasil)	PIPA (Coreia do Sul)
Autoridade de Proteção de Dados	Apresentação Unitária	Artigo 5º (XIX): "autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional"	Artigo 7º (nº1) e (nº2): "(1) A Comissão de Proteção de Informações Pessoais (doravante referida como a "Comissão de Proteção") será estabelecida pelo Primeiro-Ministro para conduzir de forma independente o trabalho relacionado com a proteção de informações pessoais. (2) A Comissão de Proteção será considerada uma agência administrativa central nos termos do Artigo 2 da Lei de Organização do Governo (...)"

Conforme o art. 5º, XIX, da LGPD, a ANPD tem poder para fazer cumprir a referida lei em todo o território nacional, podendo se afirmar que apresenta organização unitária e, não, federativa.

Nesse mesmo sentido se organiza a Comissão de Proteção, que, segundo o art. 7º (nº 2) da PIPA, é considerada agência administrativa central.

- **Quanto à qualidade jurídica**

4.2. Titulares de Dados

4.2.1. Definição

Instituição Jurídica	Subtipo de Instituição Jurídica	LGPD (Brasil)	PIPA (Coreia do Sul)
Titulares de Dados	Definição	Artigo 5º (V): "titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento"	Artigo 2º (nº3): "3. O termo 'titular dos dados' significa um indivíduo que é identificável por meio das informações processadas e é o sujeito dessas informações;"

A LGPD denomina o titular de dados apenas como “titular”, enquanto a PIPA optou por “titular dos dados”.

Conforme discutido no tópico 2.2.1 do Capítulo 2, a lei coreana considera como titular de dados o indivíduo que não só já esteja identificado, mas que também seja potencialmente identificável através do processamento de suas informações, levando-se em conta que o custo e o tempo para isso sejam razoáveis (art. 2º (nº1; b)).

No mesmo sentido, a LGPD preceitua que o titular seja a pessoa natural a quem se referem os dados pessoais objeto de tratamento, sendo que esses dados podem estar relacionados não só ao indivíduo identificado, mas também ao identificável (art. 5º, I c/c art. 5º, V).

Por isso, tanto a LGPD quanto a PIPA adotaram um entendimento expansionista de quem seja o titular de dados, ampliando o conjunto daqueles que serão protegidos por suas garantias.

4.2.2. Direito de ser informado

Instituição Jurídica	Subtipo de Instituição Jurídica	LGPD (Brasil)	PIPA (Coreia do Sul)
Titulares de Dados	Direito de Ser Informado	Artigo 6º (VI): "transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os	Artigo 4 (nº1): "O titular dos dados tem os seguintes direitos em relação ao tratamento das suas próprias informações pessoais:

		segredos comercial e industrial"	1. O direito de ser informado sobre o processamento de tais informações pessoais;"

O direito de ser informado é provido de maneira abrangente pela LGPD e pela PIPA.

O art. 6º, VI da lei brasileira estabelece que aos titulares deve ser garantida a obtenção de informações claras, precisas e facilmente acessíveis acerca do tratamento de seus dados e dos agentes que realizam esse processo.

Da mesma forma, o art. 4º (nº1) da lei coreana preceitua que ao titular é dado o direito de ser informado sobre o processamento de suas informações pessoais.

Pode-se acrescentar que, no momento do consentimento, os dois ordenamentos jurídicos mencionam a necessidade de o controlador informar ao titular o propósito do tratamento de seus dados (art. 6º, I da LGPD e art. 15 (nº2; 1) da APPI).

Por fim, reitera-se que, de acordo com a LGPD, não é possível o compartilhamento de dados pessoais com terceiros de forma oculta (FLUMIGNAN e FLUMIGNAN, 2020, p. 132). De maneira semelhante ocorre no âmbito da PIPA, segundo a qual o controlador, em regra, deve obter o consentimento do titular para fornecer informações pessoais de um sujeito a terceiro (art. 17 (nº1;1)).

4.2.3. Direito de Acesso

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**LGPD (Brasil)**	**PIPA (Coreia do Sul)**
Titulares de Dados	Direito de Acesso	Artigo 6º (IV): "livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais"	Artigo 4 (nº3): "O titular dos dados tem os seguintes direitos em relação ao tratamento das suas próprias informações pessoais: 3. O direito de confirmar se as informações pessoais estão ou não sendo processadas e de solicitar acesso (incluindo o fornecimento de cópias;

			doravante o mesmo se aplica) a essas informações pessoais;"

O direito de acesso ao tratamento de seus dados pessoais, por parte do titular, é uma garantia tanto da LGPD quanto da PIPA.

Nesse sentido, a lei coreana permite que o titular confirme se suas informações estão ou não sendo processadas, e solicite acesso a elas, podendo, inclusive, requerer o fornecimento de cópias.

A lei brasileira, do mesmo modo, confere ao titular o acesso a suas informações, podendo consultar a forma e a duração do tratamento, bem como, acerca da integralidade de seus dados.

4.2.4. Direito à Retificação

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**LGPD (Brasil)**	**PIPA (Coreia do Sul)**
Titulares de Dados	Direito à Retificação	Artigo 18 (III): "correção de dados incompletos, inexatos ou desatualizados"	Artigo 4 (nº4): "O titular dos dados tem os seguintes direitos em relação ao tratamento das suas próprias informações pessoais: 4. O direito de suspender o processamento e solicitar a correção, exclusão e destruição de tais informações pessoais;"

Conforme se verifica acima, o direito à retificação é salvaguardado, pela lei, tanto no Brasil quanto na Coreia do Sul.

Pela LGPD, o titular pode requerer do controlador a correção de seus dados que estejam incompletos, inexatos ou desatualizados.

O mesmo oferece a PIPA, segundo a qual, o titular tem o direito de corrigir suas informações pessoais.

4.2.5. Direito ao Esquecimento ou Direito ao Apagamento

Instituição Jurídica	Subtipo de Instituição Jurídica	LGPD (Brasil)	PIPA (Coreia do Sul)
Titulares de Dados	Direito ao Esquecimento ou Direito ao Apagamento	Não há previsão legal	Artigo 36 (nº1): "(1) Um titular de dados que tenha acessado suas informações pessoais nos termos do Artigo 35 pode solicitar uma correção ou apagamento de tais informações pessoais ao controlador de informações pessoais relevante: Dado que o apagamento não é permitido quando as referidas informações pessoais forem recolhidas por outros estatutos."

Nem o direito ao esquecimento, nem o direito ao apagamento são amparados pela LGPD. Na esfera da lei brasileira, somente pode se falar, conforme mencionado no tópico 2.2.5. do Capítulo 3, que o direito à eliminação (art. 18, VI) guarda similaridade com o direito ao apagamento, pela amplitude com que ao titular é autorizado requerer a eliminação de seus dados pessoais.

A PIPA, no entanto, apesar de também não garantir aos titulares o direito ao esquecimento, oferece-lhes o direito ao apagamento, pelo art. 36 (nº1). Segundo o excerto, intitulado “Retificação ou apagamento de informações pessoais”, o titular pode solicitar o apagamento de seus dados ao controlador.

4.2.6. Direito à Revogação

Instituição Jurídica	Subtipo de Instituição Jurídica	LGPD (Brasil)	PIPA (Coreia do Sul)
Titulares de Dados	Direito à Revogação	Artigo 18 (IX): "revogação do consentimento, nos termos do § 5º do art. 8º desta Lei"	Artigo 4 (nº4): "O titular dos dados tem os seguintes direitos em relação ao tratamento das suas próprias informações pessoais: 4. O direito de suspender o processamento e solicitar a

			correção, exclusão e destruição de tais informações pessoais;"

O direito à revogação (do inglês “*right to cancel*”) é resguardado tanto pela LGPD, quanto pela PIPA.

No âmbito da LGPD, essa garantia é promovida pelo art. 18, IX, sem outras delimitações restritivas (MARCACINI, 2020, p. 158). O art. 8º, § 5º, a que o preceito anterior faz menção, determina que a revogação do consentimento possa ser realizada a qualquer momento, mediante manifestação expressa do titular, levando-se em consideração que restam ratificados os tratamentos realizados sob a autorização do consentimento anterior. A oposição a esse tratamento ratificado, por sua vez, se dá pelo requerimento de eliminação desses dados pessoais restantes.

Na esfera da PIPA, o direito em tela se exprime na opção que o art. 4º (nº4) dá ao titular de suspender o tratamento e solicitar a exclusão e destruição de suas informações pessoais.

4.2.7. Direito à Limitação do Tratamento

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**LGPD (Brasil)**	**PIPA (Coreia do Sul)**
Titulares de Dados	Direito à Limitação do Tratamento	Artigo 18 (IV): "anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei"	Artigo 3º (nº1) e Artigo 4º (nº4): "(1) O controlador de informações pessoais deve tornar a finalidade do processamento de informações pessoais explícita e especificada e deve coletar o mínimo de informação pessoal, legal e justamente, na medida do necessário para tal finalidade."; "O titular dos dados tem os seguintes direitos em relação ao tratamento das suas próprias informações pessoais:

			4. O direito de suspender o processamento e solicitar a correção, exclusão e destruição de tais informações pessoais;"

O direito à limitação do tratamento de dados é uma garantia tanto da LGPD quanto da PIPA.

O art. 18, IV da LGPD preceitua que dados que sejam desnecessários ou excessivos ao cumprimento da finalidade de tratamento, ou que sejam tratados em desconformidade com o que demanda a Lei, devam ser anonimizados, bloqueados ou eliminados. Ou seja, o tratamento pode ser limitado quando o processamento for lícito, mas desnecessário ou excessivo, ou quando for ilícito (LIMA e RAMIRO, 2020, p. 259).

Por seu turno, o art. 3º (nº1) da PIPA limita o tratamento de dados ao determinar que a sua a coleta deva ser feita legal e justamente, em quantidade mínima necessária para cumprir a finalidade de tratamento. Além disso, o art. 4º (nº 4) informa que o titular tem o direito de suspender o processamento de seus dados, além de poder solicitar a correção, exclusão e destruição de tais informações pessoais.

4.2.8. Direito de Portabilidade de Dados

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**LGPD (Brasil)**	**PIPA (Coreia do Sul)**
Titulares de Dados	Direito de Portabilidade dos Dados	Artigo 18 (V): "portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial"	Não há previsão legal

Quanto ao direito à portabilidade de dados, apenas a LGPD apresenta previsão legal.

Conforme o art. 18 (V) da Lei, é permitida a portabilidade de dados a outro fornecedor de serviços ou produto mediante requisição expressa do titular. Porém, importa ressaltar que a lei não especifica o formato em que os dados devam ser transmitidos e nem a possibilidade de que ocorra uma transmissão direta entre os agentes de tratamento (LIMA e RAMIRO, 2020, p. 271).

4.2.9. Direito a Bloqueio ou Restrição do Processamento

Instituição Jurídica	Subtipo de Instituição Jurídica	LGPD (Brasil)	PIPA (Coreia do Sul)
Titulares de Dados	Direito a Bloqueio ou Restrição do Processamento	Artigo 18 (IV): "anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei"	Artigo 4º (nº4): "O titular dos dados tem os seguintes direitos em relação ao tratamento das suas próprias informações pessoais: 4. O direito de suspender o processamento e solicitar a correção, exclusão e destruição de tais informações pessoais;"

Há guarida para o direito mencionado tanto no âmbito da LGPD, quanto da PIPA.

No caso coreano, o art. 4º (nº4) permite que o titular suspenda o processamento de seus dados e solicite a correção, exclusão ou destruição de tais informações pessoais. Verifica-se que a garantia é ampla, mesmo quando detalhada nos artigos 36 e 37 da PIPA, denominados, respectivamente, “retificação ou apagamento de informações pessoais” e “suspensão do processamento de informações pessoais”.

No caso brasileiro, por sua vez, o bloqueio ou a restrição do processamento de dados é autorizado pelo art. 18, IV da Lei, quando dados desnecessários, excessivos ou tratados em desconformidade com a LGPD podem ser anonimizados, bloqueados ou eliminados.

4.2.10. Direito à Intervenção Humana na Tomada de Decisão e Criação de Perfil Automatizadas

Instituição Jurídica	Subtipo de Instituição Jurídica	LGPD (Brasil)	PIPA (Coreia do Sul)
Titulares de Dados	Direito à Intervenção Humana na Tomada de Decisão e Criação de Perfil Automatizadas	Artigo 20: "O titular dos dados tem direito a solicitar a 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"	Não há previsão legal

O direito à intervenção humana na tomada de decisão e criação de perfil automatizadas somente encontra guarida na LGPD.

Conforme já mencionado no tópico 2.2.10 do Capítulo 3, o direito à revisão das decisões automatizadas é importante para que o titular impugne erros e discriminações cometidas por algum algoritmo (SOUSA, PERRONE e MAGRANI, 2021, p. 277).

Nesse sentido, art. 20 da LGPD informa que o titular de dados pode solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado e que afetem seus interesses.

No entanto, com o veto presidencial ao § 3º do art. 20 da Lei, não há mais referência explícita à necessidade de intervenção humana nessa revisão e, consequentemente, pode ser que a decisão de um algoritmo seja revisada por outro, diminuindo-se a chance de se chegar a conclusões diferentes das apresentadas pela primeira decisão (SOUSA, PERRONE e MAGRANI, 2021, p. 277-278).

Ainda assim, pode-se falar em direito à intervenção humana na tomada de decisão e criação de perfil automatizadas pela LGPD, considerando que o texto não obsta a determinação da revisão mediante intervenção humana como

regra, na medida em que o propósito geral de transparência da Lei seria melhor cumprido dessa maneira (SOUSA, PERRONE e MAGRANI, 2021, p. 278).

Do mesmo modo, espera-se que a ANPD não fique silente sobre o tema, indicando o grau de participação humana na revisão de decisões automatizadas (SOUSA, PERRONE e MAGRANI, 2021, p. 278).

4.2.11. Limitações

Instituição Jurídica	Subtipo de Instituição Jurídica	LGPD (Brasil)	PIPA (Coreia do Sul)
Titulares de Dados	Limitações	Não há previsão legal	Artigo 58 (nº1), (nº2) e (nº3): "(1) Os capítulos 3 a 7 não se aplicam às informações pessoais indicadas em nenhum dos seguintes subparágrafos: 1. Informações pessoais coletadas pela Lei de Estatística entre informações pessoais processadas pelas instituições públicas; 2. Informações pessoais coletadas ou com o fornecimento solicitado a fim de analisar as informações relacionadas à segurança nacional; 3. Informações pessoais processadas temporariamente, caso sejam urgentemente necessárias para a segurança e bem-estar públicos, saúde pública, etc .; ou 4. Informações pessoais coletadas e usadas para seus próprios fins de comunicação pela imprensa, atividades missionárias por organizações religiosas e nomeação de candidatos por partidos políticos, respectivamente.

			(2) Os Artigos 15, 22, 27 (1) e (2), 34 e 37 não se aplicam às informações pessoais processadas por meio de dispositivos visuais de processamento de dados instalados e operados em locais abertos, nos termos de cada subparágrafo do Artigo 25 (1). (3) Os artigos 15, 30 e 31 não se aplicam às informações pessoais processadas por um controlador de informações pessoais para operar grupos ou associações de amizade, como associações de ex-alunos e clubes de hobby.";

Somente no âmbito da PIPA se evidencia um rol que limite a efetivação dos direitos de proteção de dados pessoais.

Conforme o art. 58 (nº1) da lei, não se aplicam os Capítulos 3 a 7 às informações pessoais (i) coletadas em função da Lei de Estatística; (ii) relacionadas à segurança nacional; (iii) processadas temporariamente e urgentemente para a segurança, bem-estar e saúde públicos; (iv) coletadas e usadas para fins de comunicação pela imprensa, atividade missionária por organizações religiosas e nomeação de candidatos por partidos políticos. Observa-se que os Capítulos 3 e 4 da PIPA, por exemplo, tratam, respectivamente, dos princípios de proteção de informação pessoal e dos direitos dos titulares de dados.

- **Quanto à relação jurídica entre sujeitos**

4.3. Transferência Internacional de Dados ou Processamento Transfronteiriço

A possibilidade de transferência internacional de dados pessoais está presente tanto na PIPA quanto na LGPD.

No caso da lei coreana, a previsão está no art. 17 (nº3), o qual apresenta como hipótese autorizativa de transferência a terceiro no estrangeiro apenas o consentimento do titular. Ainda assim, observa-se que a emenda nº 16.930 de agosto de 2020 modificou a PIPA como um todo, com o fim de melhor compatibiliza-la ao padrão do RGPD e, portanto, viabilizar o recebimento de decisão de adequação por parte da Comissão Europeia (KWANG HYUN RYOO, 2020).

No caso da lei brasileira, além da possibilidade de transferências internacionais pelo consentimento do titular (art. 33, VIII), também é admissível que a entrega ocorra por conta de decisão de adequação (art. 33, I) ou pela garantia, por parte do controlador, do cumprimento do regime de proteção da LGPD na forma de cláusulas contratuais específicas ou padrão (art. 33, II, “a” e “b”), de normas corporativas globais (art. 33, II, c) ou, por fim, de selos, certificados e códigos de conduta regularmente emitidos (art. 33, II, d).

4.3.1. Decisão de Adequação

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**LGPD (Brasil)**	**PIPA (Coreia do Sul)**
Transferência Internacional de Dados ou Processamento Transfronteiriço	Decisão de Adequação	Artigo 33 (I): "para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei"	Não há previsão legal

Somente no Brasil há previsão, em lei geral de proteção de dados, permitindo a transferência internacional de informações pessoais em decorrência de decisão de adequação.

Nesse sentido, consoante o art. 33, I da LGPD, estão autorizadas as transferências para países ou organismos internacionais que apresentem grau de proteção de dados pessoais adequado ao exigido pelo Brasil naquela Lei. Ainda conforme o diploma, essa avaliação será feita pela Autoridade Nacional de Proteção de Dados (art. 34, *caput*).

4.3.2. Consentimento

Instituição Jurídica	Subtipo de Instituição Jurídica	LGPD (Brasil)	PIPA (Coreia do Sul)
Transferência Internacional de Dados ou Processamento Transfronteiriço	Consentimento	Artigo 33 (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"	Artigo 17 (nº3): "(3) O controlador de informações pessoais deve informar o titular dos dados sobre as questões previstas no parágrafo (2) e obter o consentimento do titular dos dados para fornecer dados pessoais a terceiros no estrangeiro; e não deve celebrar um contrato para a transferência transfronteiriça de informações pessoais em violação desta Lei.";

O consentimento do titular é hipótese autorizativa de transferência internacional de dados pessoais tanto no Brasil quanto na Coreia do Sul.

Importa mencionar que, conforme a LGPD, art. 33, VIII, ao fornecer o seu consentimento, o titular deve estar previamente informado do caráter internacional da transferência.

O art. 17 (nº3) da PIPA, no mesmo sentido, requer que, no momento da provisão do consentimento, o titular esteja informado das questões do parágrafo nº2, mais precisamente: (i) qual o destinatário das informações pessoais; (ii) a finalidade para a qual o destinatário usa essas informações; (iii) os dados pessoais a serem fornecidos; (iv) o período durante o qual o destinatário retém e usa as informações pessoais; (v) o fato de o titular dos dados ter o direito de negar o consentimento e as desvantagens, se houver, decorrentes da negação desse consentimento.

4.3.3. Contrato

Instituição Jurídica	Subtipo de Instituição Jurídica	LGPD (Brasil)	PIPA (Coreia do Sul)
Transferência Internacional de Dados ou	Contrato	Artigo 33 (II, alíneas a e b): "quando o controlador oferecer e comprovar	Não há previsão legal

Processamento Transfronteiriço		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"	

Conforme já mencionado no tópico 2.3.3 desse capítulo, pode-se dizer que o art. 33, II da LGPD autoriza a transferência internacional de dados a controlador específico que atenda às exigências da Lei, ainda que o sistema normativo de um país ou organismo internacional terceiro não o faça (CARVALHO, 2019, p. 267).

Os incisos “a” e “b” do artigo, mais precisamente, assentem que uma transferência internacional de dados ocorra na presença de cláusulas contratuais específicas ou padrão que comprovem o respeito, por parte do controlador, aos princípios e ao regime de proteção da Lei, além dos direitos do titular.

A PIPA, no entanto, não admite tais mecanismos contratuais para anuência de transferências internacionais de dados pessoais.

4.3.4. Regras Vinculativas Aplicáveis às Empresas

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**LGPD (Brasil)**	**PIPA (Coreia do Sul)**
Transferência Internacional de Dados ou Processamento Transfronteiriço	Regras Vinculativas Aplicáveis às Empresas	Artigo 33 (II, c): "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: c) normas corporativas globais"	Não há previsão legal

Somente a LGPD permite que transferências internacionais de dados se realizem mediante o oferecimento, pelo controlador, de garantias do cumprimento do regime de proteção da Lei através de normas corporativas globais (LEONARDI, 2021, p. 305)

Reitera-se o entendimento do tópico 2.3.4 do Capítulo 3, segundo o qual as normas coorporativas globais são semelhantes às *Binding Corporate Rules* (BCRs) presentes no RGPD, que correspondem à política interna de proteção de dados das empresas de um grupo econômico, abarcando princípios, direitos dos titulares e procedimentos internos relacionados ao tema (LEONARDI, 2021, p. 305).

A expectativa é de que a ANPD seja o órgão que aprove as normas corporativas globais, conforme o que se extrai dos artigos 33, II e 36 da LGPD (LEONARDI, 2021, p. 305).

Quanto à PIPA, não há previsão de realização de transferências internacionais de dados baseadas na adoção de normas corporativas globais reconhecidas, tendo vista que os reguladores coreanos não consideraram a medida suficientemente protetiva (CHANG, 2020).

4.3.5. Certificados e Códigos de Conduta

Instituição Jurídica	**Subtipo de Instituição Jurídica**	**LGPD (Brasil)**	**PIPA (Coreia do Sul)**
Transferência Internacional de Dados ou Processamento Transfronteiriço	Certificados e Códigos de Conduta	Artigo 33 (II, d): "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: d) selos, certificados e códigos de conduta regularmente emitidos"	Não há previsão legal

Por fim, a LGPD também autoriza a realização de transferências internacionais de dados pessoais por controladores que apresentarem selo,

certificado ou código de conduta reconhecido pela ANPD, comprovando obedecer ao regime de proteção da Lei (LEONARDI, 2021, p. 305).

A PIPA, por outro lado, não reconhece tal mecanismo para a tutela de dados a serem transferidos a terceiro no estrangeiro.

5. Conclusões acerca das principais divergências e convergências entre a LGPD e a PIPA

Em primeiro lugar, quanto à autoridade nacional de proteção de dados, tanto o Brasil quanto o Coreia apresentam órgãos independentes e unitários, sendo eles, respectivamente, a Autoridade Nacional de Proteção de Dados (ANPD) e a Comissão de Proteção de Informações Pessoais (Comissão de Proteção). Reitera-se que, conforme se examinou no tópico 2.1.1. desse capítulo, a autonomia da ANPD é formal, sendo, na prática, dependente da disposição da administração direta em pouco ingerir nas atividades do órgão.

Em segundo lugar, no que diz respeito aos direitos dos titulares, tanto no Brasil quanto na Coreia se adota um conceito expansionista de quem sejam os titulares de dados, ampliando-se o número daqueles que são destinatários das garantias oferecidas por suas leis de proteção de dados.

Quanto aos direitos dos titulares de dados, especificamente, percebe-se que ambos os sistemas normativos procuram resguardá-los de forma satisfatória. Nesse sentido, das 10 (dez) categorias relacionadas a direitos de titulares apresentadas entre os tópicos 3.2.2 e 3.2.11 do Capítulo 3, em 6 (seis) delas, tanto o Brasil quanto a Coreia do Sul ostentam previsão legal; em 2 (duas), somente o Brasil prevê alguma garantia; e, em 2 (duas), somente a Coreia do Sul se manifesta.

Mais precisamente quanto às coincidências, a LGPD e a APPI promovem adequadamente a seus titulares, ainda que, quanto a uma ou outra categoria, haja diferença na amplitude da garantia, o direito de: (i) ser informado; (ii) de acesso; (iii) à retificação; (iv) à revogação; (v) à limitação do tratamento; e, (vi) a bloqueio ou restrição do processamento. Observa-se que são as mesmas categorias que estão presentes tanto no ordenamento brasileiro, quanto no japonês, conforme o tópico 3 do presente capítulo.

Ainda quanto aos direitos dos titulares, no que se refere às divergências entre LGPD e PIPA, somente o Brasil prevê o direito de portabilidade de dados e o direito à intervenção humana na tomada de decisão e criação de perfil automatizadas. Por outro lado, somente na Coreia do Sul pode se falar em direito ao apagamento e em um rol de limites aplicados aos direitos dos titulares.

Em terceiro lugar, no que se refere à transferência internacional de dados, das 5 categorias de autorização elencadas entre os tópicos 3.3.1 e 3.3.5 desse capítulo, existe 1 (uma) aplicada pelos dois países e 4 (quatro) apresentadas somente pelo Brasil.

Assim, a legislação coreana prevê que uma transferência internacional de dados pessoais ocorra apenas mediante o consentimento do titular, hipótese encontrada também na LGPD. No entanto, apesar da escassez de circunstâncias autorizativas observada na PIPA, pode-se falar que o país resguarda seus titulares no que diz respeito a transferências internacionais de dados, tendo em vista que o consentimento é a forma mais elementar de proteção.

No entanto, se não é possível afirmar que esse cenário acarrete necessariamente em prejuízo à proteção dos dados de um titular, pode-se dizer que um modelo que apresente mais hipóteses de transferência de informações pessoais a terceiro no exterior proporcionaria maior atuação dos atores econômicos nacionais a nível global diante de uma economia altamente digitalizada.

Enfim, verifica-se que a LGPD apresenta 4 (quatro) outras hipóteses de autorização para transferências internacionais de dados. São elas (i) a consolidação de decisão de adequação entre Brasil e outro país ou organismo internacional; (ii) a comprovação pelo controlador do respeito aos princípios e direitos da Lei, através de cláusulas contratuais específicas ou padrão; (iii) a mesma comprovação, pelo controlador, por meio de normas corporativas globais; e, por fim, (iv) a mesma comprovação, pelo controlador, a partir de selos, certificados e códigos de conduta regularmente emitidos.

Ao final, por meio da análise realizada pela ótica do modelo TLICS nos tópicos 4.1, 4.2 e 4.3 desse capítulo, identificou-se inúmeras congruências entre o sistema normativo brasileiro e o coreano, no que diz respeito à existência de uma autoridade de proteção de dados independente, ao oferecimento de amplas

garantias aos titulares e à regulamentação de transferências internacionais de dados. Conclui-se, desse modo, que há comensurabilidade entre a LGPD e a PIPA, de forma que a transferência de dados pessoais entre Coreia do Sul e o Brasil é segura.

CONCLUSÃO

A presente monografia teve como objetivo identificar o grau de comensurabilidade entre a Lei nº 13.709/18, ou Lei Geral de Proteção de Dados Pessoais (LGPD), a Lei sobre a Proteção de Informações Pessoais do Japão (APPI) e a Lei de Proteção de Informações Pessoais da Coreia do Sul (PIPA).

Essa comparação se operou pela aplicação do Modelo TLICS, o qual permite identificar quais garantias institucionais para proteção de dados pessoais estão presentes na LGPD, na APPI e na PIPA, de forma a se definir o grau de compatibilidade entre os diplomas na tarefa de resguardar seus titulares em meio a transferências internacionais de dados entre os países.

Assim, dos 51 subtipos de variáveis jurídicas presentes no modelo, 18 foram selecionados em decorrência da necessidade de apresentar as variáveis mais representativas em formato passível de compreensão quando da comparação das três leis.

As variáveis escolhidas dizem respeito, assim, (i) à autonomia/independência da autoridade de proteção de dados; (ii) à apresentação da autoridade, se federativa ou unitária; (iii) à definição de quem seja o titular de dados pessoais; (iv) ao direito de ser informado; (v) ao direito de acesso; (vi) ao direito à retificação; (vii) ao direito ao esquecimento ou ao apagamento; (viii) ao direito à revogação; (ix) ao direito à limitação do tratamento; (x) ao direito à portabilidade dos dados; (xi) ao direito ao bloqueio ou restrição do processamento; (xii) ao direito à intervenção humana na tomada de decisão e criação de perfil automatizadas; (xiii) à limitação a esses direitos; à autorização de transferências internacionais de dados mediante (xiv) decisão de adequação; (xv) consentimento; (xvi) contrato; (xvii) regras vinculativas aplicáveis às empresas; ou (xviii) certificados e códigos de conduta.

Da investigação, materializada nos Capítulos 2 e 3 desse trabalho, quanto à presença ou ausência das variáveis supracitadas na LGPD, na PIPA e na APPI, identificou-se que os 3 (três) países apresentam arcabouço jurídico suficientemente protetivo para seus titulares, inclusive em meio a transferências internacionais de dados pessoais. Isso se deve à presença de autoridades nacionais de proteção de dados independentes, ainda que, no Brasil, somente do ponto de vista formal; ao reconhecimento de numerosos direitos de proteção

de dados para o titular; e, da tutela direcionada a dados pessoais transferidos internacionalmente.

Concluiu-se, portanto, que há comensurabilidade entre as leis gerais de proteção de dados pessoais do Brasil e do Japão e do Brasil e da Coreia do Sul, o que significa que a transferência de dados pessoais entre o Brasil e esses dois países ocorreria de maneira segura.

A expectativa, a partir dessa conclusão, é de que o Brasil se incorpore cada vez mais à sociedade da informação, ao ampliar seu fluxo de dados com outros países.

REFERÊNCIAS BIBLIOGRÁFICAS

ANJOS, L. Decisões automatizadas e transparência algorítimica. **Instituto de Referência em Internet e Sociedade**, 06 nov. 2019. Disponivel em: <https://irisbh.com.br/decisoes-automatizadas-e-transparencia-algoritmica/>.

ARANHA, M. I. et al. Comparative Analysis between Personal Data Legal Protection: A Methodological Approach. **Communication Policy Research Latin America**, Cordoba, Argentina, v. 13, p. 141-162, 2019.

ARANHA, M. I. et al. Data Protection Authority Influence on the Rights of Data Subjects and other Data Protection Legal Institutions in Latin America. **Communication Policy Research Latin America**, 2020.

ARANHA, M. I.; OLIVEIRA, F. M. G. S. **ICT Institutional Framework:** Americas Region ICT Federal Index. 1º. ed. Londres: Laccademia Publishing Limited, 2016.

BIONI, B. R. **Proteção de dados pessoais:** a função e os limites do consentimento. 2ª. ed. Rio de Janeiro: Forense, 2020.

BIONI, B.; FAVARO, I.; RIELLI, M. Porque a transferência internacional de dados tem que ser segura? **Observatório por DataPrivacyBR**, 05 out. 2020. Disponivel em: <https://observatorioprivacidade.com.br/2020/10/05/por-que-a-transferencia-internacional-de-dados-tem-que-ser-segura/>.

CARVALHO, A. G. P. D. Transferência internacional de dados na lei geral de proteção de dados - Força normativa e efetividade diante do cenário transnacional. In: FRAZÃO, A., et al. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Revista dos Tribunais, 2019.

CASTELLS, M. **A Sociedade em Rede**. 8ª. ed. São Paulo: Paz e Terra, v. I, A Era da Informação: Economia, Sociedade e Cultura, 2005.

CHANCE, C. Amendments to the Protection of Personal Information Act of Japan, jun. 2020. Disponivel em: <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2020/06/amendments-to-the-%20protection-of-personal-information-act-of-japan.pdf>.

CHANG, K. &. Data Protected - Republic of Korea. **Linklaters**, mar. 2020. Disponivel em: <https://www.linklaters.com/pt-br/insights/data-protected/data-protected---republic-of-korea>.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez 2011.

DONEDA, D. A Autoridade Nacional de Proteção de Dados e o Conselho Nacional de Proteção de Dados. In: DANILO DONEDA, I. W. S. L. S. M. O. L. R. J. E. B. R. B. **(Coord.) Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense , 2021. Cap. 23, p. 466-476.

EUROPEIA, C. **Comunicação da Comissão ao Parlamento Europeu e ao Conselho:** Intercâmbio e proteção de dados pessoais num mundo globalizado. Bruxelas: Bélgica. 2017. p. 18.

EUROPEIA, C. **Decisão de Execução (UE) 2019/419**. [S.l.]: [s.n.]. 2019a.

EUROPEIA, C. Joint Statement by Commissioner Reynders and Yoon Jong In, Chairperson of the Personal Information Protection Commission of the Republic of Korea. **European Comission**, Bruxelas, 30 mar. 2021. Disponivel em: <https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1506>.

EUROPEU, P. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**. Bruxelas. 2016.

FLUMIGNAN, S. J. G.; FLUMIGNAN, W. G. G. Princípios que regem o tratamento de dados no Brasil. In: LIMA, C. R. P. D. **Comentários à Lei Geral de Proteção de Dados coord.** São Paulo: Almedina Brasil, 2020. Cap. 5, p. 123-140.

FONSECA, H. M. A interpretação da constituição: o método "hermenêutico-concretizador" de Konrad Hesse. **Revista do Tribunal Regional do Trabalho da 13ª Região**, João Pessoa, v. 13, p. 158-182, 2005. Disponivel em: <http://bdjur.stj.jus.br/dspace/handle/2011/18159>.

GARFINKEL, S. **Database Nation:** the death of privacy in the 21st Century. 1ª. ed. [S.l.]: O'Reilly, 2000.

HOUNSLOW, D.; NOZAKI, R. Japan - Data Protection Overview. **DataGuidance**, jul. 2020. Disponivel em: <https://www.dataguidance.com/notes/japan-data-protection-overview>.

ISHIARA, T. Japan. **The Privacy, Data Protection and Cybersecurity Law Review**, London, n. 7º, p. 263-282, 2020. Disponivel em: <https://www.sidley.com/-/media/publications/the-privacy-data-protection-and-cybersecurity-law-review-2020-japan.pdf?la=en>.

KWANG BAE PARK, J. Y. Y. J. K. J. B. J. H. K. H. K. K. S. C. T. J. K. M. K. K. M. S. Major Amendment to the Personal Information Protection Act Passed by National Assembly. **Newsletter: Data Privacy & Cybersecurity Group**, jan. 2020. Disponivel em: <http://www.leeko.com/newsl/dpc/202001_1/e/dpc202001_e.html>.

KWANG HYUN RYOO, J. Y. M. Y. J. E. P. Data Protection & Privacy 2020. **Chambers and Partners**, Seoul, 09 mar. 2020. Disponivel em: <https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2020/south-korea/trends-and-developments>.

LEME, C. D. S. Proteção e tratamento de dados sob o prisma da legislação vigente. **Fronteiras Interdisciplinares do Direito**, v. 1, n. 1, p. 178-197, 2019. Acesso em: 08 maio 2020.

LEONARDI, M. Transferência Internacional de Dados Pessoais. In: DONEDA, D., et al. **(Coord.) Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. Cap. 14.

LIMA, C. R. P. D. O conceito de tratamento de dados após o caso Google Spain e sua influência na sociedade brasileira. **III Encontro de Internacionalização do CONPEDI**, v. 09, p. 117-140, 2015. Acesso em: 08 maio 2020.

LIMA, C. R. P. D.; PEROLI, K. A Aplicação da Lei Geral de Proteção de Dados do Brasil no Tempo e no Espaço. In: COORD., C. R. P. D. L. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020. p. 69-99.

LIMA, C. R. P. D.; RAMIRO, L. F. M. Direitos do Titular dos Dados Pessoais. In: COORD., C. R. P. D. L. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina Brasil, 2020. p. 249-277.

MACIEL, R. Os perigos da ditadura pelos dados. **Consultor Jurídico**, 2020. Disponivel em: <https://www.conjur.com.br/2020-mai-04/rafael-maciel-perigos-ditadura-pelos-dados?imprimir=1>. Acesso em: 07 maio 2020.

MAÑAS, J. L. P. El derecho fundamental a la protección de los datos personales. **IV Encuentro Iberoamericano de Proteccíon de Datos Personales**, México, n. 1ª, p. 17-41, 2005. Disponivel em: <http://www.transparencia.udg.mx/sites/default/files/IV%20Encuentro%20Iberoamericano%20de%20protecci%C3%B3n%20de%20datos%20personales%20en%20M%C3%A9xico.pdf>. Acesso em: 15 jun. 2020.

MARCACINI, A. T. R. Regras aplicadas ao tratamento de dados pessoais. In: LIMA, C. R. P. D. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020. Cap. 6, p. 141-161.

MENDES, L. S. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. **Jota**, 10 maio 2020. Disponivel em: <https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020>. Acesso em: 17 jun. 2020.

MENDES, L. S.; DONEDA, D. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, 120, nov-dez 2018. 469-483.

PALHARES, F. Revisão de decisões automatizadas. **Jota**, 29 set. 2019. Disponivel em: <https://www.jota.info/opiniao-e-analise/artigos/revisao-de-decisoes-automatizadas-29092019>.

PALMER, R. E. **Hermenêutica**. Lisboa: Edições 70, 1969.

PESSÔA, L. C. **A Teoria da Interpretação Jurídica de Emilio Betti**. Porto Alegre: Sergio Antonio Fabris Editor, 2002.

PEZZENELLA, M. C. C.; WENCZENOVICZ, T. J. Bancos de dados, conhecimento e redes científicas: a visibilidade na sociedade da informação. **III**

Encontro de Internacionalização do CONPEDI, v. 1, n. 9, p. 102-116, 2015. Acesso em: 08 maio 2020.

ROCHFELD, J. Como qualificar os dados pessoais? Uma perspectiva teórica e normativa da União Europeia em face dos gigantes da Internet. **Revista de Direito, Estado e Telecomunicações**, Brasília, v. 10, n. 1, p. 61-84, 2018. Disponivel em: <https://periodicos.unb.br/index.php/RDET/article/view/21500/19816>. Acesso em: 04 maio 2020.

ROESLER, C. R. A tiologia da interpretação de Emilio Betti. **Revista Direito Em Debate**, v. 7, n. 11, p. 7-46, 1998.

SARLET, G. B. S.; CALDEIRA, C. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. **Civilistica**, Rio de Janeiro, n. 1, 2019. Disponivel em: <http://civilistica.com/o-consentimento-informado-e-a-protecao/>. Acesso em: 04 maio 2020.

SCHERTEL, L. **Privacidade, proteção de dados e defesa do consumidor:** Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

SOUSA, C. A.; PERRONE, C.; MAGRANI, E. O direito à explicação entre a experiência europeia e a sua positivação na LGPD. In: MENDES, L. S., et al. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Editora Forense, 2021.

SPAREMBERGER, R. F. L. Betti x Gadamer: Da hermenêutica objetivista à hermenêutica criativa. **Revista da Faculdade de Direito da Universidade Federal do Paraná**, v. 39, n. 0, p. 171-189, 2003.

STRECK, L. L. **Hermenêutica Jurídica em Crise**. 3ª. ed. Porto Alegre: Livraria do Advogado, 2001.

TAKASE, K. GDPR matchup: Japan's Act on the Protection of Personal Information. **Iapp**, 29 ago. 2017. Disponivel em: <https://iapp.org/news/a/gdpr-matchup-japans-act-on-the-protection-of-personal-information/>.

VERONESE, A. Transferências internacionais de dados pessoais: o debate transatlântico norte e sua repercussão na América Latina e no Brasil. In: DONEDA, D., et al. **(Coord.) Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. Cap. 35.

WHON-IL, P. Recent amendments to PIPA. **Korean LII**, 15 maio 2020. Disponivel em: <http://koreanlii.or.kr/w/index.php/Recent_amendments_to_PIPA>.

Anexo 1

Tabela comparativa entre a APPI (Japão) e a PIPA (Coreia do Sul), pela ótica dos 51 subtipos de instituições jurídicas do Modelo TLICS.

	Instituição Jurídica	Subtipo de Instituição Jurídica	APPI (Japão)	PIPA (Coreia do Sul)
Entidade Jurídica	**Autoridade de Proteção de Dados**	**Autônoma/ Independente**	Artigo 59 (nº2) e artigo 62: "(2) A Comissão pertence à jurisdição do Primeiro Ministro"; "O presidente e os comissários da Comissão devem exercer a sua autoridade oficial de forma independente".	Artigo 7º (nº1) e (nº2): "(1) A Comissão de Proteção de Informações Pessoais (doravante referida como a "Comissão de Proteção") será estabelecida pelo Primeiro-Ministro para conduzir de forma independente o trabalho relacionado com a proteção de informações pessoais. (2) A Comissão de Proteção será considerada uma agência administrativa central nos termos do Artigo 2 da Lei de Organização do Governo (...)"
		Não Autônoma/ Não Independente		
		Apresentação Federativa		
		Apresentação Unitária	Artigo 59 (nº2): "(2) A Comissão pertence à jurisdição do Primeiro-Ministro."	Artigo 7º (nº1) e (nº2): "(1) A Comissão de Proteção de Informações Pessoais (doravante referida como a "Comissão de Proteção") será estabelecida pelo Primeiro-Ministro para conduzir de forma independente o trabalho relacionado com a proteção de informações pessoais. (2) A Comissão de Proteção será considerada uma agência administrativa central nos termos do Artigo 2 da Lei de Organização do Governo (...)"
	Conselho de Proteção de Dados			
Qualidade Jurídica	**Titulares de Dados**	**Definição**	Artigo 2º (nº 8): "(8) Um 'titular' de informações pessoais, nesta Lei, significa um indivíduo específico identificável por informações pessoais"	Artigo 2º (nº3): "3. O termo 'titular dos dados' significa um indivíduo que é identificável por meio das informações processadas e é o sujeito dessas informações;"
		Direito de Ser Informado	Artigo 27 (nº1; i a iv): "(1) Um PIHBO, em relação às informações pessoais retidas por si, disponibilizará os tópicos descritos a seguir de forma que o titular possa conhecê-los (incluindo aqueles casos em que, a pedido de um titular, responderá sem demora). (i) o nome ou denominação e endereço e, para uma pessoa jurídica, o nome de seu representante, do referido PIHBO (ii) a finalidade de utilização de todos os dados pessoais retidos (excluindo-se os casos abrangidos pelo item (i) ao item (iii) do artigo 18, parágrafo (4)) (iii) os procedimentos para responder a uma solicitação, nos termos do parágrafo seguinte, ou a uma demanda, nos termos do Artigo seguinte, parágrafo (1) (incluindo como aplicado mutatis mutandis nos termos do Artigo seguinte, parágrafo (5)); Artigo 29, parágrafo (1); ou Artigo 30, parágrafo (1), parágrafo (3) ou parágrafo (5) (incluindo, quando o valor de uma taxa tiver sido decidido de acordo com o disposto no artigo 33, parágrafo (2), o valor da taxa) (iv) além dos estabelecidos nos três itens anteriores, aqueles prescritos por decreto ministerial como um assunto necessário para garantir o manuseio adequado dos dados pessoais retidos"	Artigo 4 (nº1): "O titular dos dados tem os seguintes direitos em relação ao tratamento das suas próprias informações pessoais: 1. O direito de ser informado sobre o processamento de tais informações pessoais;"
		Direito de Acesso	Artigo 28 (nº1): "(1) Um titular pode exigir de um PIHBO a divulgação de dados pessoais retidos que possam identificar ele ou ela por um método de fornecimento de registro eletromagnético ou outros métodos prescritos pelas regras da Comissão de Proteção de Informações Pessoais."	Artigo 4 (nº3): "O titular dos dados tem os seguintes direitos em relação ao tratamento das suas próprias informações pessoais: 3. O direito de confirmar se as informações pessoais estão ou não sendo processadas e de solicitar acesso (incluindo o fornecimento de cópias; doravante o mesmo se aplica) a essas informações pessoais;"
		Direito à Retificação	Artigo 29 (nº1): "(1) Um titular pode, quando o conteúdo de dados pessoais retidos que podem identificá-lo não estiver exato, exigir que um PIHBO faça uma correção, adição ou exclusão (de agora em diante denominada "correção etc." no presente artigo) em relação ao conteúdo dos dados pessoais retidos."	Artigo 4 (nº4): "O titular dos dados tem os seguintes direitos em relação ao tratamento das suas próprias informações pessoais: 4. O direito de suspender o processamento e solicitar a correção, exclusão e destruição de tais informações pessoais;"

Direito ao Esquecimento ou Direito ao Apagamento		Artigo 36 (nº1): "(1) Um titular de dados que tenha acessado suas informações pessoais nos termos do Artigo 35 pode solicitar uma correção ou apagamento de tais informações pessoais ao controlador de informações pessoais relevante: Dado que o apagamento não é permitido quando as referidas informações pessoais forem recolhidas por outros estatutos."
Direito à Revogação	Artigo 30 (nº1) e (nº5): "(1) Um titular pode, quando dados pessoais retidos que podem identificá-lo estão sendo tratados em violação às disposições do Artigo 16 ou Artigo 16-2, ou, foram adquiridos em violação às disposições do Artigo 17, exigir de um PIHBO a cessação da utilização ou eliminação (doravante referida como "cessação da utilização etc." neste Artigo) dos dados pessoais retidos."; "(5) Um titular pode exigir que o PIHBO cumpra uma cessação de utilização etc. dos dados pessoais retidos, ou cesse uma provisão a terceiros, se tiver se tornado desnecessário para PIHBO utilizar dados pessoais retidos que possam identificar o titular, se uma situação prescrita na cláusula principal do Artigo 22-2, parágrafo (1) ocorreu em conexão com os dados pessoais retidos que possam identificar o titular, ou existe a possibilidade de que o tratamento dos dados pessoais retidos que possam identificar o titular prejudiquem os direitos ou interesses legítimos desse."	Artigo 4 (nº4): "O titular dos dados tem os seguintes direitos em relação ao tratamento das suas próprias informações pessoais: 4. O direito de suspender o processamento e solicitar a correção, exclusão e destruição de tais informações pessoais;"
Direito à Limitação do Tratamento	Artigo 16 (nº1), Artigo 29 (nº1) e Artigo 30 (nº1) e (nº5): "(1) Um PIHBO não deve tratar informações pessoais, sem obter previamente o consentimento do titular, para além do âmbito necessário para cumprir uma finalidade de utilização especificada de acordo com o disposto no artigo anterior."; "(1) Um titular pode, quando o conteúdo de dados pessoais retidos que podem identificá-lo não estiver exato, exigir que um PIHBO faça uma correção, adição ou exclusão (de agora em diante denominada "correção etc." no presente artigo) em relação ao conteúdo dos dados pessoais retidos."; "(1) Um titular pode, quando dados pessoais retidos que possam identificá-lo estão sendo tratados em violação às disposições do Artigo 16 ou Artigo 16-2, ou, foram adquiridos em violação às disposições do Artigo 17, exigir de um PIHBO a cessação da utilização ou eliminação (doravante referida como "cessação da utilização etc." neste Artigo) dos dados pessoais retidos."; "(5) Um titular pode exigir que o PIHBO cumpra uma cessação de utilização etc. dos dados pessoais retidos, ou cesse uma provisão a terceiros, se tiver se tornado desnecessário para PIHBO utilizar dados pessoais retidos que possam identificar o titular, se uma situação prescrita na cláusula principal do Artigo 22-2, parágrafo (1) ocorreu em conexão com os dados pessoais retidos que possam identificar o titular, ou existe a possibilidade de que o tratamento dos dados pessoais retidos que possam identificar o titular prejudiquem os direitos ou interesses legítimos desse."	Artigo 3º (nº1) e Artigo 4º (nº4): "(1) O controlador de informações pessoais deve tornar a finalidade do processamento de informações pessoais explícita e especificada e deve coletar o mínimo de informação pessoal, legal e justamente, na medida do necessário para tal finalidade."; "O titular dos dados tem os seguintes direitos em relação ao tratamento das suas próprias informações pessoais: 4. O direito de suspender o processamento e solicitar a correção, exclusão e destruição de tais informações pessoais;"
Direito de Portabilidade dos Dados		

	Direito a Bloqueio ou Restrição do Processamento	Artigo 29 (nº1) e Artigo 30 (nº1) e (nº5): "(1) Um titular pode, quando o conteúdo de dados pessoais retidos que podem identificá-lo não estiver exato, exigir que um PIHBO faça uma correção, adição ou exclusão (de agora em diante denominada "correção etc." no presente artigo) em relação ao conteúdo dos dados pessoais retidos."; "(1) Um titular pode, quando dados pessoais retidos que possam identificá-lo estão sendo tratados em violação às disposições do Artigo 16 ou Artigo 16-2, ou, foram adquiridos em violação às disposições do Artigo 17, exigir de um PIHBO a cessação da utilização ou eliminação (doravante referida como “cessação da utilização etc.” neste Artigo) dos dados pessoais retidos."; "(5) Um titular pode exigir que o PIHBO cumpra uma cessação de utilização etc. dos dados pessoais retidos, ou cesse uma provisão a terceiros, se tiver se tornado desnecessário para PIHBO utilizar dados pessoais retidos que possam identificar o titular, se uma situação prescrita na cláusula principal do Artigo 22-2, parágrafo (1) ocorreu em conexão com os dados pessoais retidos que possam identificar o titular, ou existe a possibilidade de que o tratamento dos dados pessoais retidos que possam identificar o titular prejudiquem os direitos ou interesses legítimos desse."	Artigo 4 (nº4): "O titular dos dados tem os seguintes direitos em relação ao tratamento das suas próprias informações pessoais: 4. O direito de suspender o processamento e solicitar a correção, exclusão e destruição de tais informações pessoais;"
	Direito à Intervenção Humana na Tomada de Decisão e Criação de Perfil Automatizadas		
	Limitações		Artigo 58 (nº1), (nº2) e (nº3): "(1) Os capítulos 3 a 7 não se aplicam às informações pessoais indicadas em nenhum dos seguintes subparágrafos: 1. Informações pessoais coletadas pela Lei de Estatística entre informações pessoais processadas pelas instituições públicas; 2. Informações pessoais coletadas ou com o fornecimento solicitado a fim de analisar as informações relacionadas à segurança nacional; 3. Informações pessoais processadas temporariamente, caso sejam urgentemente necessárias para a segurança e bem-estar públicos, saúde pública, etc .; ou 4. Informações pessoais coletadas e usadas para seus próprios fins de comunicação pela imprensa, atividades missionárias por organizações religiosas e nomeação de candidatos por partidos políticos, respectivamente. (2) Os Artigos 15, 22, 27 (1) e (2), 34 e 37 não se aplicam às informações pessoais processadas por meio de dispositivos visuais de processamento de dados instalados e operados em locais abertos, nos termos de cada subparágrafo do Artigo 25 (1). (3) Os artigos 15, 30 e 31 não se aplicam às informações pessoais processadas por um controlador de informações pessoais para operar grupos ou associações de amizade, como associações de ex-alunos e clubes de hobby.";
Operador			

	Controlador		Artigo 2º (nº5), (nº10) e (nº12), Artigo 26-2 (nº1): "(5) Um **'operador comercial responsável pelo tratamento de informações pessoais'**, nesta Lei, significa uma pessoa que fornece um banco de dados de informações pessoais, etc. para utilização na atividade comercial (...)"; "(10) Um **'operador comercial responsável pelo tratamento de informações processadas de forma pseudônima'**, nesta Lei, significa uma pessoa que fornece para uso nos negócios uma coletividade de informações compreendendo informações processadas de forma pseudônima que foram sistematicamente organizadas (...)"; "(12) Um '**operador comercial responsável pelo tratamento de informações processadas de forma anônima**', nesta Lei, significa uma pessoa que fornece para uso em negócios uma coletividade de informações compreendendo informações processadas anonimamente que foram sistematicamente organizadas (...)" "(1) **Um operador comercial responsável pelo tratamento de informações pessoalmente referenciáveis** (ou seja, uma pessoa que fornece um banco de dados de informações pessoalmente referenciáveis etc. (...)";	Artigo 2º (nº5): "5. O termo 'controlador de informações pessoais' significa uma instituição pública, pessoa jurídica, organização, indivíduo, etc. que processa informações pessoais direta ou indiretamente para operar os arquivos de informações pessoais como parte de suas atividades;"
	Órgão de Pesquisa			
	Encarregado			
Objeto Jurídico	**Dados Pessoais**		Artigo 2º (nº1; i e ii), (nº2), (nº6) e (nº7) e Artigo 26-2 (nº1): "(1) "**Informações pessoais**", nesta Lei, significa as informações relativas a um indivíduo vivo que se enquadram em qualquer um dos seguintes itens: (i) aqueles que contenham um nome, data de nascimento ou outras descrições, etc. (significando toda e qualquer questão (excluindo um código de identificação individual) declarada, gravada ou expressa de outra forma usando voz, movimento ou outros métodos em um documento, desenho ou registro eletromagnético (significando um registro mantido sob forma eletromagnética (significando formas eletrônicas, magnéticas ou outras que não podem ser reconhecidas pelos sentidos humanos; o mesmo se aplica no próximo parágrafo, item (ii)); o mesmo se aplica no Artigo 18, parágrafo (2) e Artigo 28, parágrafo (1)); daqui em diante o mesmo), pelo qual um indivíduo específico pode ser identificado (incluindo aqueles que podem ser facilmente agrupados com outras informações e, assim, identificar um indivíduo específico) (ii) aqueles que contêm um código de identificação individual"; "(2) Um "**código de identificação individual**", nesta Lei, significa aqueles prescritos por ordem de gabinete, os quais são qualquer caractere, letra, número, símbolo ou outro código abrangido por qualquer um dos itens a seguir."; "(6) "**Dados pessoais**", nesta Lei, significa informações pessoais que constituem um banco de dados de informações pessoais etc."; "(7) "**Dados pessoais retidos**" nesta Lei significa os dados pessoais que um PIHBO tem autoridade para divulgar, corrigir, adicionar ou excluir o conteúdo, cessar a utilização, apagar e cessar o fornecimento a terceiros, e que devem não ser aquelas prescritas por decreto ministerial como susceptíveis de prejudicar o público ou outros interesses se sua presença ou ausência for divulgada."; "(1) (...) uma coletividade de informações que inclui **informações pessoalmente referenciáveis** (ou seja, informações relacionadas a um indivíduo vivo que não se enquadram em informações pessoais, informações processadas de forma pseudônima ou informações processadas de forma anônima; (...)"	Artigo 2º (nº1; a, b e c): "Os termos usados nesta Lei serão definidos da seguinte forma: 1. O termo "informações pessoais" significa qualquer uma das seguintes informações relacionadas com um indivíduo vivo: (a) Informações que identificam um determinado indivíduo por seu nome completo, número de registro de residente, imagem, etc .; (b) Informações que, mesmo que por si só não identifiquem um determinado indivíduo, podem ser facilmente combinados com outras informações para identificar um determinado indivíduo. Em tais casos, se há ou não facilidade de combinação deve ser determinado considerando razoavelmente o tempo, custo, tecnologia, etc. usados para identificar o indivíduo, assim como a probabilidade de que outras informações possam ser obtidas; (c) Informações nos itens (a) ou (b) acima que são pseudonimizadas de acordo com o subparágrafo 1-2 abaixo e, portanto, torna-se incapaz de identificar um indivíduo particular sem o uso ou combinação de informações para restauração ao estado original (doravante denominado "informação pseudonimizada");"

	Dados Pessoais Sensíveis		Artigo 2º (nº3): "(3) 'Informações pessoais que requerem atenção especial', nesta Lei, significa informações pessoais que compreendem a raça, o credo, o status social, o histórico médico e os antecedentes criminais, bem como o fato de ter sofrido danos em consequência de um crime, ou outras descrições, etc. determinadas por decreto ministerial como aquelas cujo tratamento exige atenção especial para não causar discriminação injusta, preconceito ou outras desvantagens ao titular."	Artigo 23 (nº1): "(1) O controlador de informações pessoais não deve processar as informações pessoais (de agora em diante denominadas "dados sensíveis") incluindo ideologia, crença, admissão em/saída de sindicatos ou partidos políticos, pensamento político, saúde, vida sexual e outras informações pessoais que provavelmente estão prejudicando a privacidade dos titulares de dados, conforme prescrito pelo Decreto Presidencial; (...)"
	Banco de Dados		Artigo 2º (nº4) e Artigo 26-2 (nº1): "(4) Um 'banco de dados de informações pessoais, etc.', nesta Lei, significa aqueles estabelecidos a seguir, que são um conjunto coletivo de informações que compreende informações pessoais (excluindo as prescritas por decreto ministerial como tendo pouca possibilidade de prejudicar os direitos e interesses de um indivíduo, considerando seu método de utilização)"; "(1) (...) banco de dados de informações pessoalmente referenciáveis etc. (ou seja, uma coletividade de informações que inclui informações pessoalmente referenciáveis (...)"	Artigo 2º (nº4): "4. O termo 'arquivo de informações pessoais' significa um conjunto ou conjuntos de informações pessoais dispostas ou organizadas de maneira sistemática com base em uma determinada regra para facilitar a busca das informações pessoais;"
	Avaliação de Impacto			Artigo 33 (nº1), (nº2) e (nº8): "(1) No caso de haver risco de violação das informações pessoais dos titulares dos dados devido à operação de arquivos de informações pessoais que atendam aos critérios prescritos pelo Decreto Presidencial, o chefe de uma instituição pública deve realizar uma avaliação para analisar os fatores de risco e melhorá-los (doravante designada por "avaliação de impacto na privacidade") e submeter os seus resultados à Comissão de Proteção. Nesses casos, o chefe da instituição pública deve solicitar a avaliação de impacto na privacidade de qualquer uma das instituições designadas pela Comissão de Proteção (doravante referido como "instituição AIP")."; "(2) A Avaliação de Impacto à Privacidade deve abranger os assuntos dos seguintes subparágrafos: 1. O número de informações pessoais sendo processadas; 2. Se as informações pessoais são fornecidas a terceiros ou não; 3. A probabilidade de violar os direitos dos titulares dos dados e o grau desse risco; e 4. Os outros assuntos conforme prescritos pelo Decreto Presidencial."; "(8) O controlador de informações pessoais que não seja a instituição pública deve realizar esforços de maneira positiva para conduzir a Avaliação de Impacto à Privacidade, se a violação de informações pessoais de titulares de dados for altamente provável na operação dos arquivos de informações pessoais."
	Âmbito Territorial			
	Âmbito Material		Artigo 1º: "Esta lei visa proteger os direitos e interesses de um indivíduo, considerando a utilidade das informações pessoais, incluindo que a aplicação adequada e eficaz das informações pessoais contribui para a criação de novas indústrias e a realização de uma sociedade econômica vibrante e uma qualidade de vida enriquecida para o povo do Japão; estabelecendo a visão geral para o manuseio adequado das informações pessoais, criando uma política básica governamental com relação a isso e estabelecendo outros assuntos para servir de base para medidas que visam proteger as informações pessoais, bem como esclarecendo as responsabilidades etc. dos governos central e local e estabelecendo obrigações etc. que um PIHBO deve cumprir, à luz da utilização significativamente expandida de informações pessoais à medida que nossa sociedade evolui, baseada em informação e comunicação avançadas."	Artigo 6º: "A proteção de dados será regida por esta lei, exceto quando especificamente previsto em outras leis."

Status Jurídico	**Fundamentos Jurídicos para o Tratamento de Dados Pessoais**	**Consentimento**	Artigo 16 (nº1): "(1) Um PIHBO não deve tratar informações pessoais, sem obter previamente o consentimento do titular, para além do âmbito necessário para cumprir uma finalidade de utilização especificada de acordo com o disposto no artigo anterior."	Artigo 4º (nº2): "O titular dos dados deve, em relação ao processamento de suas próprias informações pessoais, ter os direitos estabelecidos nos seguintes parágrafos: 2. O direito de consentir ou não, e de eleger o escopo do consentimento, para o processamento de tais informações pessoais;"
		Execução de um Contrato		Artigo 15 (nº1; 4): "(1) O controlador de informações pessoais pode coletar informações pessoais em qualquer um dos seguintes casos e usá-las dentro do escopo das finalidades de coleta: 4. Onde for inevitavelmente necessário, a fim de executar e realizar um contrato com os titulares dos dados;"
		Obrigação Jurídica	Artigo 16 (nº3; i): "(3) As disposições dos dois parágrafos anteriores não se aplicarão aos casos descritos a seguir. (i) casos baseados em leis e regulamentos";"	Artigo 15 (nº1; 2): "(1) O controlador de informações pessoais pode coletar informações pessoais em qualquer um dos seguintes casos e usá-las dentro do escopo das finalidades de coleta: 2. Quando existirem disposições especiais em leis ou for inevitável, a fim de observar obrigações legais;"
		Proteção dos Interesses Vitais do Titular de Dados ou de outra Pessoa Natural	Artigo 16 (nº3; ii): "(3) As disposições dos dois parágrafos anteriores não se aplicarão aos casos descritos a seguir. (ii) casos em que há necessidade de proteger a vida humana, a integridade física ou bens e que seja difícil obter o consentimento do titular"	Artigo 15 (nº1; 5): "(1) O controlador de informações pessoais pode coletar informações pessoais em qualquer um dos seguintes casos e usá-las dentro do escopo das finalidades de coleta: 5. Quando julgar necessária explicitamente a proteção, contra riscos iminentes, da vida, integridade física ou lucro econômico do titular dos dados ou de terceiros, caso o titular dos dados ou seu representante legal não estejam em condições de expressar intenção, ou não é possível obter consentimento prévio devido a endereços desconhecidos; ou"
		Interesse Público	Artigo 16 (nº3; iv): "(3) As disposições dos dois parágrafos anteriores não se aplicarão aos casos descritos a seguir. (iv) casos em que é necessário cooperar com agências ou organismos governamentais ou com os seus representantes na execução das suas tarefas legais, e quando haja a possibilidade de que a obtenção do consentimento do titular interfira na execução de tais tarefas";"	Artigo 15 (nº1; 3): "(1) O controlador de informações pessoais pode coletar informações pessoais em qualquer um dos seguintes casos e usá-las dentro do escopo das finalidades de coleta: 3. Quando for inevitável para que a instituição pública possa realizar esse trabalho sob sua jurisdição, conforme prescrito por leis e regulamentos;"
		Interesse Legítimo		Artigo 15 (nº1; 6): "(1) O controlador de informações pessoais pode coletar informações pessoais em qualquer um dos seguintes casos e usá-las dentro do escopo das finalidades de coleta: 6. Quando for necessário atingir o interesse justificável do controlador de informações pessoais, o qual seja explicitamente superior ao dos titulares dos dados. Nesse caso, é permitido apenas quando existe uma relação substancial com o interesse justificável do controlador de informações pessoais e não excede o escopo razoável."
		Propósito de Pesquisa	Artigo 76 (nº1; iii): "(1) Para uma pessoa estabelecida em cada item a seguir que seja um PIHBO, as disposições do Capítulo IV não se aplicarão quando o todo ou parte da finalidade de tratamento de informações pessoais etc. for uma finalidade prescrita em cada item mencionado respectivamente. (iii) uma universidade e outra organização ou grupo voltado para estudos acadêmicos ou uma pessoa pertencente a eles: a finalidade de ser fornecida para uso em estudos acadêmicos."	Artigo 28-2 (nº1): "(1) Um controlador de informações pessoais pode processar informações pseudonimizadas sem o consentimento dos titulares dos dados para fins estatísticos, de pesquisa científica e de arquivamento de interesse público, etc."

		Exercício Regular de Direitos em Processo Judicial		Artigo 18 (nº2; 7 a 9): "(2) Não obstante o parágrafo (1), onde qualquer um dos seguintes subparágrafos se aplica, um controlador de informações pessoais pode usar informações pessoais ou fornecê-las a terceiros para outros fins, a menos que isso seja susceptível de infringir injustamente o interesse dos titulares de dados ou de terceiros (...): 7. Onde for necessário para a investigação de crimes, indiciamento e processo criminal; 8. Quando for necessário que um tribunal prossiga com os deveres relacionados com o julgamento; 9. Quando for necessário para a aplicação da pena, liberdade condicional e custódia."
		Proteção à Saúde	Artigo 16 (nº3; iii): "(3) As disposições dos dois parágrafos anteriores não se aplicarão aos casos descritos a seguir. (iii) casos em que há uma necessidade especial de melhorar a salubridade pública ou promover o crescimento de crianças saudáveis e que seja difícil obter o consentimento do titular"	
		Proteção do Crédito		
		Acesso Público		
		Anonimização		Artigo 58-2: "Esta lei não se aplica a informações que não identifiquem mais um determinado indivíduo quando combinadas com outras informações, considerando razoavelmente o tempo, custo, tecnologia, etc."
		Registro Civil		
	Fundamentos Jurídicos para o Tratamento de Dados Pessoais Sensíveis	**Consentimento Específico - Consentimento Explícito - Consentimento Distinto**	Artigo 17 (nº2): "(2) Um PIHBO, exceto nos casos estabelecidos a seguir, não adquirirá informações pessoais que requerem atenção especial sem obter previamente o consentimento do titular"	Artigo 23 (nº1; 1): "(1) O controlador de informações pessoais não deve processar as informações pessoais (daqui em diante denominadas "dados sensíveis"), (...); previsto, no entanto, que o mesmo não deve se aplicar quando qualquer um dos subparágrafos a seguir for aplicável: 1. Quando o controlador de informações pessoais informa os titulares de dados acerca de cada subparágrafo do artigo 15(2) ou 17(2), e obtém o consentimento dos titulares de dados separadamente do consentimento para outro processamento de informações pessoais;"
		Obrigação Jurídica	Artigo 17 (nº2; i): "(2) Um PIHBO, exceto nos casos estabelecidos a seguir, não adquirirá informações pessoais que requerem atenção especial sem obter previamente o consentimento do titular. (i) casos baseados em leis e regulamentos"	Artigo 23 (nº1; 2): "(1) O controlador de informações pessoais não deve processar as informações pessoais (daqui em diante denominadas "dados sensíveis"), (...); previsto, no entanto, que o mesmo não deve se aplicar quando qualquer um dos subparágrafos a seguir for aplicável: 2. Quando leis e regulamentos exigem, ou permitem, o processamento de dados sensíveis."
		Interesse Público	Artigo 17 (nº2; iv): "(2) Um PIHBO, exceto nos casos estabelecidos a seguir, não adquirirá informações pessoais que requerem atenção especial sem obter previamente o consentimento do titular. (iv) casos em que é necessário cooperar com agências ou organismos governamentais ou com os seus representantes na execução das suas tarefas legais, e quando haja a possibilidade de que a obtenção do consentimento do titular interfira na execução de tais tarefas"	
		Estudos		
		Exercício Regular de Direitos em Processo Judicial		

		Proteção da Vida ou da Segurança Física do Titular de Dados	Artigo 17 (nº2; ii): "(2) Um PIHBO, exceto nos casos estabelecidos a seguir, não adquirirá informações pessoais que requerem atenção especial sem obter previamente o consentimento do titular. (ii) casos em que há necessidade de proteger a vida humana, a integridade física ou bens e que seja difícil obter o consentimento do titular"	
		Proteção da Saúde	Artigo 17 (nº2; iii): "(2) Um PIHBO, exceto nos casos estabelecidos a seguir, não adquirirá informações pessoais que requerem atenção especial sem obter previamente o consentimento do titular. (iii) casos em que há uma necessidade especial de melhorar a salubridade pública ou promover o crescimento de crianças saudáveis e que seja difícil obter o consentimento do titular"	
		Prevenção à Fraude		
	Dado Anonimizado, Bloqueado ou Apagado		Artigo 2º (nº 9) e (nº11): "(9) '**Informações processadas de forma pseudônima**' neste Ato significa informações relativas a um indivíduo que podem ser produzidas a partir do processamento de informações pessoais, de modo a não ser capaz de identificar um indivíduo específico, a menos que comparadas com outras informações por meio da ação prescrita em cada item a seguir em concordância com as divisões de informações pessoais estabelecidas em cada um desses itens."; "(11) '**Informações processadas de forma anônima**' nesta Lei significa informações relativas a um indivíduo que podem ser produzidas a partir do processamento de informações pessoais, de modo que não seja capaz de identificar um indivíduo específico (...) nem ser capaz de restaurar as informações pessoais."	
Relação Jurídica entre Sujeitos	**Transferência Internacional de Dados ou Processamento Transfronteiriço**	**Decisão de Adequação**	Artigo 24 (nº1): "(1) Um PIHBO, com exceção daqueles casos previstos em cada item do artigo anterior, parágrafo (1), deverá, no caso de fornecer dados pessoais a um terceiro (excluindo-se uma pessoa que estabeleça um sistema em conformidade aos padrões prescritos pelas regras da Comissão de Proteção de Informações Pessoais, conforme necessário para a tomada contínua de ações equivalentes àquelas que um PIHBO deve adotar em relação ao tratamento de dados pessoais, de acordo com as disposições desta Seção (referida como "ação equivalente" no parágrafo (3)); doravante o mesmo neste parágrafo, no parágrafo seguinte e no Artigo 26-2, parágrafo (1), item (ii)) em um país estrangeiro (significando um país ou região localizado fora do território do Japão; a seguir, o mesmo) (**excluindo-se aqueles prescritos pelas regras da Comissão de Proteção de Informações Pessoais como um país estrangeiro que estabeleça um sistema de proteção de informações pessoais reconhecido como tendo um padrão equivalente ao do Japão em relação à proteção dos direitos e interesses de um indivíduo; a seguir, o mesmo neste Artigo, no parágrafo seguinte e no Artigo 26-2, parágrafo (1), item (ii)**), obter previamente o consentimento do titular no sentido de que ele ou ela aprove o fornecimento a um terceiro em país estrangeiro. Nesse caso, o previsto no Artigo anterior não se aplica"	

		Consentimento	Artigo 24 (nº1): "(1) Um PIHBO, com exceção daqueles casos previstos em cada item do artigo anterior, parágrafo (1), deverá, no caso de fornecer dados pessoais a um terceiro (excluindo-se uma pessoa que estabeleça um sistema em conformidade aos padrões prescritos pelas regras da Comissão de Proteção de Informações Pessoais, conforme necessário para a tomada contínua de ações equivalentes àquelas que um PIHBO deve adotar em relação ao tratamento de dados pessoais, de acordo com as disposições desta Seção (referida como "ação equivalente" no parágrafo (3)); doravante o mesmo neste parágrafo, no parágrafo seguinte e no Artigo 26-2, parágrafo (1), item (ii)) em um país estrangeiro (significando um país ou região localizado fora do território do Japão; a seguir, o mesmo) (excluindo-se aqueles prescritos pelas regras da Comissão de Proteção de Informações Pessoais como um país estrangeiro que estabeleça um sistema de proteção de informações pessoais reconhecido como tendo um padrão equivalente ao do Japão em relação à proteção dos direitos e interesses de um indivíduo; a seguir, o mesmo neste Artigo, no parágrafo seguinte e no Artigo 26-2, parágrafo (1), item (ii)), **obter previamente o consentimento do titular no sentido de que ele ou ela aprove o fornecimento a um terceiro em país estrangeiro**. Nesse caso, o previsto no Artigo anterior não se aplica"	Artigo 17 (nº3): "(3) O controlador de informações pessoais deve informar o titular dos dados sobre as questões previstas no parágrafo (2) e obter o consentimento do titular dos dados para fornecer dados pessoais a terceiros no estrangeiro; e não deve celebrar um contrato para a transferência transfronteiriça de informações pessoais em violação desta Lei."
		Contrato	Artigo 24 (nº1): "(1) Um PIHBO, com exceção daqueles casos previstos em cada item do artigo anterior, parágrafo (1), deverá, no caso de fornecer dados pessoais a um terceiro (**excluindo-se uma pessoa que estabeleça um sistema em conformidade aos padrões prescritos pelas regras da Comissão de Proteção de Informações Pessoais, conforme necessário para a tomada contínua de ações equivalentes àquelas que um PIHBO deve adotar em relação ao tratamento de dados pessoais, de acordo com as disposições desta Seção (referida como "ação equivalente" no parágrafo (3)); doravante o mesmo neste parágrafo, no parágrafo seguinte e no Artigo 26-2, parágrafo (1), item (ii)**) em um país estrangeiro (significando um país ou região localizado fora do território do Japão; a seguir, o mesmo) (excluindo-se aqueles prescritos pelas regras da Comissão de Proteção de Informações Pessoais como um país estrangeiro que estabeleça um sistema de proteção de informações pessoais reconhecido como tendo um padrão equivalente ao do Japão em relação à proteção dos direitos e interesses de um indivíduo; a seguir, o mesmo neste Artigo, no parágrafo seguinte e no Artigo 26-2, parágrafo (1), item (ii)), obter previamente o consentimento do titular no sentido de que ele ou ela aprove o fornecimento a um terceiro em país estrangeiro. Nesse caso, o previsto no Artigo anterior não se aplica"	
		Regras Vinculativas Aplicáveis às Empresas	Artigo 24 (nº1): "(1) Um PIHBO, com exceção daqueles casos previstos em cada item do artigo anterior, parágrafo (1), deverá, no caso de fornecer dados pessoais a um terceiro (**excluindo-se uma pessoa que estabeleça um sistema em conformidade aos padrões prescritos pelas regras da Comissão de Proteção de Informações Pessoais, conforme necessário para a tomada contínua de ações equivalentes àquelas que um PIHBO deve adotar em relação ao tratamento de dados pessoais, de acordo com as disposições desta Seção (referida como "ação equivalente" no parágrafo (3)); doravante o mesmo neste parágrafo, no parágrafo seguinte e no Artigo 26-2, parágrafo (1), item (ii)**) em um país estrangeiro (significando um país ou região localizado fora do território do Japão; a seguir,	

			ou região localizado fora do território do Japão; a seguir, o mesmo) (excluindo-se aqueles prescritos pelas regras da Comissão de Proteção de Informações Pessoais como um país estrangeiro que estabeleça um sistema de proteção de informações pessoais reconhecido como tendo um padrão equivalente ao do Japão em relação à proteção dos direitos e interesses de um indivíduo; a seguir, o mesmo neste Artigo, no parágrafo seguinte e no Artigo 26-2, parágrafo (1), item (ii)), obter previamente o consentimento do titular no sentido de que ele ou ela aprove o fornecimento a um terceiro em país estrangeiro. Nesse caso, o previsto no Artigo anterior não se aplica"	
		Certificados e Códigos de Conduta	Artigo 24 (nº1): "(1) Um PIHBO, com exceção daqueles casos previstos em cada item do artigo anterior, parágrafo (1), deverá, no caso de fornecer dados pessoais a um terceiro (**excluindo-se uma pessoa que estabeleça um sistema em conformidade aos padrões prescritos pelas regras da Comissão de Proteção de Informações Pessoais, conforme necessário para a tomada contínua de ações equivalentes àquelas que um PIHBO deve adotar em relação ao tratamento de dados pessoais, de acordo com as disposições desta Seção (referida como "ação equivalente" no parágrafo (3)); doravante o mesmo neste parágrafo, no parágrafo seguinte e no Artigo 26-2, parágrafo (1), item (ii)**) em um país estrangeiro (significando um país ou região localizado fora do território do Japão; a seguir, o mesmo) (excluindo-se aqueles prescritos pelas regras da Comissão de Proteção de Informações Pessoais como um país estrangeiro que estabeleça um sistema de proteção de informações pessoais reconhecido como tendo um padrão equivalente ao do Japão em relação à proteção dos direitos e interesses de um indivíduo; a seguir, o mesmo neste Artigo, no parágrafo seguinte e no Artigo 26-2, parágrafo (1), item (ii)), obter previamente o consentimento do titular no sentido de que ele ou ela aprove o fornecimento a um terceiro em país estrangeiro. Nesse caso, o previsto no Artigo anterior não se aplica"	
	Uso Compartilhado de Dados Pessoais			
	Responsabilidade e Ressarcimento de Danos			Artigo 4º (nº5) e Artigo 39 (nº1): "O titular dos dados deve, em relação ao processamento de suas próprias informações pessoais, ter os direitos estabelecidos nos seguintes parágrafos: 5. O direito a reparação adequada por qualquer dano decorrente do processamento dessas informações pessoais em um procedimento rápido e justo."; "(1) Qualquer titular de dados que sofra danos causados pelo controlador de informações pessoais em violação a esta Lei pode reivindicar os danos contra o controlador de informações pessoais. Nesse caso, o referido controlador de informações pessoais não poderá ser exonerado da responsabilidade por danos se não provar a inexistência de sua intenção ou negligência ilícitas."
	Sanções Administrativas		Artigo 88: "Uma pessoa abrangida por qualquer um dos itens a seguir será punida com uma multa não criminal de não mais que 100.000 ienes. (i) uma pessoa que violou o disposto no Artigo 26, parágrafo (2) (incluindo-se conforme aplicado mutatis mutandis nos termos do Artigo 26-2, parágrafo (3)), ou no Artigo 55 (ii) uma pessoa que não apresentou uma notificação ou que enviou falsamente uma notificação nos termos do Artigo 50, parágrafo (1)"	Artigo 75 (nº5): "(5) As multas administrativas previstas nos parágrafos (1) a (4) serão impostas e cobradas pela Comissão de Proteção e pelo chefe de uma agência administrativa central relacionada, conforme prescrito por Decreto Presidencial. (...)"

urídica entre Sujeito	**Tratamento de Dados**			Artigo 2º (nº2): "2. O termo 'processamento' significa a coleta, geração, conexão, intertravamento, gravação, armazenamento, retenção, processamento de valor agregado, edição, pesquisa, saída, correção, recuperação, uso, fornecimento, divulgação e destruição de informações pessoais e outras atividades semelhantes;"
	Tratamento de Dados Sensíveis			Artigo 23: "(1) O controlador de informações pessoais não deve processar as informações pessoais (de agora em diante denominadas "dados sensíveis") incluindo ideologia, crença, admissão em/saída de sindicatos ou partidos políticos, pensamento político, saúde, vida sexual e outras informações pessoais que provavelmente estão prejudicando a privacidade dos titulares de dados, conforme prescrito pelo Decreto Presidencial; previsto, no entanto, que o mesmo não deve se aplicar quando qualquer um dos subparágrafos a seguir for aplicável:"
	Tratamento de Dados de Crianças e Adolescentes	**De 12 anos**		Artigo 22 (nº6): "(6) Quando for necessário obter o consentimento, nos termos desta Lei, para processar informações pessoais de uma criança menor de 14 anos de idade, um controlador de informações pessoais deve obter o consentimento do seu representante legal. Nesses casos, mínimas informações pessoais necessárias para obter o consentimento do representante legal podem ser coletadas diretamente dessa criança, sem o consentimento de seu representante legal."
		De 13 anos		Artigo 22 (nº6): "(6) Quando for necessário obter o consentimento, nos termos desta Lei, para processar informações pessoais de uma criança menor de 14 anos de idade, um controlador de informações pessoais deve obter o consentimento do seu representante legal. Nesses casos, mínimas informações pessoais necessárias para obter o consentimento do representante legal podem ser coletadas diretamente dessa criança, sem o consentimento de seu representante legal."
		De 14 anos		
		De 15 anos		
		De 16 anos		
	Tratamento de Dados por Autoridades Públicas			
	Anonimização		Artigo 2º (nº11): "(11) 'Informações processadas de forma anônima' nesta Lei significa informações relativas a um indivíduo que podem ser produzidas a partir do processamento de informações pessoais, de modo que não seja capaz de identificar um indivíduo específico (...) nem ser capaz de restaurar as informações pessoais."	Artigo 2 (nº1-2) e Artigo 28-5 (nº1): "1-2. O termo 'pseudonimização' significa um procedimento para processar informações pessoais de forma que as informações não possam identificar um determinado indivíduo sem informações adicionais, excluindo parcialmente ou substituindo no todo ou em parte, tais informações;"; "(1) Ninguém deve processar as informações pseudonimizadas com o objetivo de identificar um determinado indivíduo."
	Obrigações do Controlador de Dados	**Segurança de Dados**	Artigo 20: "Um PIHBO deve tomar as medidas necessárias e apropriadas para o controle de segurança dos dados pessoais, incluindo a prevenção de vazamentos, perdas ou danos em relação a esses dados pessoais tratados"	Artigo 3º (nº4) e Artigo 29: "(4) O controlador de informações pessoais deve gerenciar as informações pessoais de maneira segura, de acordo com os métodos, tipos, etc. de processamento de informações pessoais, considerando a possibilidade de que os direitos do titular sejam violados e o grau de tal risco."; "O controlador de informações pessoais deve tomar medidas técnicas, administrativas e físicas, como plano de gerenciamento interno e preservação de registros de logon, etc., necessárias para garantir a segurança especificada pelo Decreto Presidencial, para que as informações pessoais não sejam perdidas, roubadas, vazadas, forjadas, alteradas ou danificadas."

		Notificação de Violação de Dados	Artigo 22-2 (nº1) e (nº2): "(1) Um PIHBO deverá, de acordo com as regras da Comissão de Proteção de Informações Pessoais, relatar à Comissão de Proteção de Informações Pessoais quando houver vazamento, perda ou danos ou outra situação relativa à garantia de segurança de seus dados pessoais processados, sendo prescritos pelas regras da Comissão de Proteção de Informações Pessoais como aqueles em relação aos quais existe uma grande possibilidade de prejudicar os direitos e interesses de um indivíduo. Isto, no entanto, não se aplica nos casos em que o referido PIHBO confiado por outro PIHBO da totalidade ou parte do referido tratamento de dados pessoais informou a ocorrência de tal situação ao referido PIHBO conforme prescrito pelas regras da Comissão de Proteção de Informações Pessoais."; "(2) Nos casos previstos no parágrafo anterior, um PIHBO (excluindo-se aqueles que informaram nos termos do disposto no parágrafo anterior) deve, de acordo com as regras da Comissão de Proteção de Dados Pessoais, notificar o titular da ocorrência da referida situação. Isto, entretanto, não se aplica quando for difícil informar um titular e quando medidas alternativas necessárias forem tomadas para proteger os direitos e interesses do titular."	Artigo 34 (nº1; 1 a 5): "(1) O controlador de informações pessoais deve notificar os titulares de dados prejudicados, sem demora, dos fatos dos subparágrafos a seguir, quando souber que informações pessoais vazaram: 1. Que tipo de informação pessoal vazou; 2. Quando e como as informações pessoais vazaram; 3. Quaisquer informações sobre como os titulares dos dados podem fazer para minimizar os possíveis danos sofridos pelo vazamento de informações pessoais; 4. Contramedidas do controlador de informações pessoais e procedimentos de correção; e 5. Suporte técnico do controlador de informações pessoais e pontos de contato para os titulares de dados relatarem problemas."
		Encarregado pelo Tratamento de Dados		Artigo 31 (nº1): "O controlador de informações pessoais deve designar um oficial de privacidade que se responsabilize de forma abrangente pelo processamento de informações pessoais"
		Proteção de Dados por Defeitos		
		Proteção de Dados desde a Concepção		
	Mecanismos de Governança e de Prestação de Contas		Artigo 47 (nº1): "(1) Uma corporação (incluindo um organismo não corporativo que nomeou um representante ou administrador; o mesmo se aplicará no Artigo seguinte, item (iii), (b)) que pretende prestar os seguintes serviços, a fim de garantir o manuseio adequado das informações pessoais etc. (excluindo-se informações pessoalmente referenciáveis; doravante o mesmo se aplica nesta Seção) por um PIHBO etc. (excluindo-se PRIHBO; doravante, o mesmo se aplica nesta Seção), pode receber um credenciamento da Comissão de Proteção de Informações Pessoais."	Artigo 30 (nº1) e Artigo 61 (nº2): "(1) O controlador de informações pessoais deve estabelecer a política de processamento de informações pessoais, incluindo os itens dos subparágrafos a seguir (daqui em diante denominada "Política de Privacidade"). Nesse caso, as instituições públicas devem estabelecer a Política de Privacidade para os arquivos de informações pessoais a serem registrados nos termos do artigo 32:"; "(2) A Comissão de Proteção pode aconselhar um controlador de informações pessoais a melhorar o status do processamento de informações pessoais quando isso for considerado necessário para proteger as informações pessoais. Nesses casos, ao receber o conselho, o controlador de informações pessoais deve aplicar esforços sinceros para cumprir o conselho e informar a Comissão de Proteção dos resultados."