Pontifícia Universidade Católica de São Paulo
PUC-SP

Marília Machado Muchiuti

Do RGPD à LGPD: difusão internacional de normas e o caso das regulamentações de proteção de dados pessoais

Mestrado Profissional em Governança Global e Formulação de Políticas Internacionais

São Paulo
2022

Pontifícia Universidade Católica de São Paulo
PUC-SP

Marília Machado Muchiuti

Do RGPD à LGPD: difusão internacional de normas e o caso das regulamentações de proteção de dados pessoais

Dissertação apresentada à Banca Examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para a obtenção do título de MESTRE PROFISSIONAL em Governança Global e Formulação de Políticas Internacionais, sob orientação do Prof. Dr. Luiz Guilherme Arcaro Conci

São Paulo
2022

Sistemas de Bibliotecas da Pontifícia Universidade Católica de São Paulo -
Ficha Catalográfica com dados fornecidos pelo autor

Muchiuti, Marília Machado
Do RGPD à LGPD: Difusão internacional de normas e o caso das regulamentações de proteção de dados pessoais / MaríliaMachado Muchiuti. -- São Paulo: [s.n.], 2022.
75p ; cm.

Orientador: Luiz Guilherme Arcaro Conci.
Trabalho Final (Mestrado Profissional) -- Pontifícia Universidade Católica de São Paulo, Programa de Estudos Pós-Graduados em Governança Global e Formulação de Políticas Internacionais, 2022.

1. Difusão internacional de normas. 2. Proteção de dados pessoais. 3. Relações Internacionais. 4. Direito. I. Conci, Luiz Guilherme Arcaro. II. Pontifícia Universidade Católica de São Paulo, Mestrado Profissional em Governança Global e Formulação de Políticas Internacionais. III. Título.

CDD

Marília Machado Muchiuti

Do RGPD à LGPD: difusão internacional de normas e o caso das regulamentações de proteção de dados pessoais

Dissertação apresentada à Banca Examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para a obtenção do título de MESTRE PROFISSIONAL em Governança Global e Formulação de Políticas Internacionais, sob orientação do Prof. Dr. Luiz Guilherme Arcaro Conci

Aprovada em: _____/_____/_____

BANCA EXAMINADORA

_____

Prof. Dr. Luiz Guilherme Arcaro Conci

_____

Profa. Dra. Clarisse Laupman Ferraz Lima

_____

Prof. Dr. Andriei da Cunha Guerrero Gutierrez

AGRADECIMENTOS

Aos meus pais, Renato e Eloísa, pelo trabalho árduo que permitiu que eu construísse meus próprios caminhos, mas sempre com o conforto da lembrança de que nunca estarei desamparada.

Ao meu orientador, pelo apoio e paciência durante a elaboração deste trabalho.

Aos professores e amigos da PUC-SP que me acompanharam durante o programa de mestrado em Governança Global e Formulação de Políticas Internacionais. Obrigada pelas valiosas lições, por tornarem essa trajetória mais leve e por ampliarem a minha visão por vezes legalista.

A todos os colegas de trabalho que tive nos departamentos jurídicos e escritórios de advocacia dos quais fiz e faço parte, bem como ao Mackenzie, instituição à qual estive vinculada durante quase toda minha vida escolar e universitária. Todos foram essenciais para que eu pudesse experienciar o nexo entre vida acadêmica e prática profissional que se reflete na conclusão deste mestrado.

RESUMO

Este trabalho busca tratar o fenômeno da difusão, analisando os processos e as forças por meio das quais normas então restritas a determinada localidade acabam por penetrar ordenamentos de outras localidades, difundindo-se globalmente. A análise é realizada a partir do estudo do caso da difusão de normas que regulamentam a proteção de dados pessoais, mais particularmente a difusão do Regulamento Geral sobre a Proteção de Dados da União Europeia de 2016 (RGPD), até o Brasil, o qual adotou uma Lei Geral de Proteção de Dados Pessoais em 2018 (LGPD). Para isso, a análise é principalmente feita sob a perspectiva da teoria do "Efeito Bruxelas" da autora Anu Bradford – a qual busca explicar a forma com a qual a União Europeia é capaz de exportar normas facilitadas por mercados, empresas privadas e dinâmicas de influência – e recorre principalmente aos recursos de investigação do processo legislativo da LGPD, bem como de análise do conteúdo da LGPD em comparação ao teor normativo do RGPD. Com os resultados desta análise, o trabalho acaba por debater como o processo de difusão de normas no sistema internacional tem o potencial de romper com as visões tradicionais desse sistema, aproximando perspectivas e literaturas das Relações Internacionais e do Direito para uma compreensão holística e integrada.

Palavras-chave: difusão internacional de normas; proteção de dados pessoais; Relações Internacionais; Direito.

ABSTRACT

This work seeks to address the phenomenon of diffusion, analyzing the processes and forces through which norms initially restricted to a certain location end up penetrating other locations, spreading globally. The analysis is based in the case study of diffusion of norms that regulate the protection of personal data, more particularly the diffusion of European Union's General Data Protection Regulation of 2016 (RGPD), to Brazil, which adopted a General Personal Data Protection Act in 2018 (LGPD). For this purpose, the analysis is mainly based on the "Brussels Effect" theory by author Anu Bradford – which seeks to explain European Union's ability is exporting norms facilitated by markets, private companies, and dynamics of influence – and mainly uses the legislative process of the LGPD, as well as the content of the LGPD in comparison to the normative content of the RGPD, as its investigative resources. With the results of this analysis, the work finally debates how the process of diffusion of norms in the international system has the potential to disrupt traditional views of this system, bringing together perspectives and literatures of International Relations and Law for a holistic and integrated approach.

Palavras-chave: international diffusion of norms; personal data protection; International Relations; Law.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABA	Associação Brasileira de Anunciantes
ABAP	Associação Brasileira de Agências de Publicidade
ABCD	Associação Brasileira de Crédito Digital
ABDOH	Associação Brasileira Mídia Out Of Home
ABEMD	Associação Brasileira de Marketing Direto
ABERT	Associação Brasileira das Empresas de Rádio e Televisão
ABES	Associação Brasileira das Empresas Software
ABINEE	Associação Brasileira da Indústria Elétrica e Eletrônica
ABRANET	Associação Brasileira de Internet
ABRARC	Associação Brasileira de Auditoria, Gestão de Riscos & Compliance
ABRASEM	Associação Brasileira de Sementes e Mudas
ABRATEL	Associação Brasileira de Rádio e Televisão
ANBC	Associação Nacional dos Bureaus de Crédito
ANER	Associação Nacional de Editores de Revistas
ANID	Associação Nacional para Inclusão Digital
ANJ	Associação Nacional de Jornais
ANPD	Autoridade Nacional de Proteção de Dados
APP	Associação dos Profissionais de Propaganda
APPI	*Act on the Protection of Personal Information*
ARPEN	Associação Nacional dos Registradores de Pessoas Naturais
ASBRAAP	Associação Brasileira de Agricultura de Precisão e Digital
ASSESPRO	Associação das Empresas Brasileiras de Tecnologia da Informação
BRASILCON	Instituto Brasileiro de Política e Direito do Consumidor
BRASSCOM	Presidente da Associação Brasileira de Empresas de Tecnologia da Informação e Comunicação
CACB	Confederação das Associações Comerciais e Empresariais do Brasil
CAMARA-E.NET	Câmara Brasileira de Comércio Eletrônico
CAMP	Clube Associativo dos Profissionais de Marketing Político

CCTCI	Comissão de Ciência e Tecnologia, Comunicação e Informática
CDC	Código de Defesa do Consumidor
CTS/FGV	Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas
DEM-RJ	Partido Democratas – Rio de Janeiro
DPO	*Data Protection Officer*
EBC	Empresa Brasileira de Comunicação
FECOMERCIOSP	Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo
FENAINFO	Federação Nacional da Empresas de Informática
FENAPRO	Federação Nacional das Agências de Propaganda
FNDC	Fórum Nacional pela Democratização da Comunicação
IAB	*Interactive Advertising Bureau*
IBDDIG	Instituto Brasileiro De Direito Digital
IDEC	Instituto Brasileiro de Defesa do Consumidor
IDP	Instituto Brasiliense de Direito Público
LGPD	Lei Geral de Proteção de Dados Pessoais
MBC	Movimento Brasil Competitivo
MPDFT	Ministério Público do Distrito Federal e Territórios
P&D BRASIL	Associação de Empresas de Desenvolvimento Tecnológico Nacional e Inovação
PCDOB-SP	Partido Comunista do Brasil – São Paulo
PDT-CE	Partido Democrático Trabalhista – Ceará
PL	Projeto de Lei
PRB-SP	Partido Republicano Brasileiro – São Paulo
PSD-GO	Partido Social Democrático do Goiás
PSD-RJ	Partido Social Democrático do Rio de Janeiro
PT-AC	Partido dos Trabalhadores – Acre
RGPD	Regulamento Geral sobre a Proteção de Dados
SEINESP	Sindicato das Empresas de Internet do Estado de São Paulo
SENACON/MJ	Secretaria Nacional do Consumidor do Ministério da Justiça
SEPROSP	Sindicato das Empresas de Processamento de Dados e Serviços de Informática do Estado de São Paulo
TIC	Tecnologia da Informação e das Comunicações

UE	União Europeia
USP	Universidade de São Paulo

SUMÁRIO

1 INTRODUÇÃO

A sociedade do século XXI, inserida em um mundo globalizado e altamente conectado, é capaz de fazer com que decisões tomadas em determinados territórios causem impactos e desdobramentos em outras partes do mundo, em países ou locais que, a princípio, são soberanos, autônomos e independentes. Essa espécie de “efeito borboleta” das relações internacionais explicita que ações locais, ainda que restritas a um país ou fórum específico, repercutem globalmente, em outros níveis ou jurisdições. Para fins didáticos, a expressão “difusão” ou “transferência” é utilizada neste trabalho para nomear esse movimento.

Embora a difusão não seja um fenômeno exclusivamente recente, o contexto da Era da Informação contribui para a sua intensificação em virtude da superação de barreiras geográficas em maior escala e maior velocidade. Na prática, isso é evidenciado pelos avanços tecnológicos que facilitam fluxos de pessoas, mercadorias, capitais, bens, serviços e informações que fazem surgir novas preocupações e debates entre diversos atores da sociedade.

Como outros conflitos sociais que precisam ser ponderados, essas preocupações e debates acabam exigindo negociações, moderações e até mesmo regulamentações que, por sua vez, também estão sujeitas a serem difundidas globalmente. Este cenário é evidente, por exemplo, no caso dos debates e regulamentações acerca da proteção de dados pessoais, que acabaram se difundindo por diferentes países no decorrer dos anos e, mais intensamente, por volta de 2016.

Assim, o fenômeno da difusão reflete em diferentes campos de estudo, sobretudo nas áreas das Relações Internacionais, por tratar das dinâmicas entre os diversos atores que compõem o sistema internacional, e do Direito, por tratar da transferência de normas e imposição de direitos e obrigações advindos de diferentes sistemas jurídicos. Fato é que, diante das dinâmicas expostas acima, a ordem internacional e jurídica que conhecemos – e que colocam o Estado em uma posição quase exclusiva de governança – estão mudando, urgindo a análise e interpretação dessas dinâmicas sob um olhar holístico e atualizado.

É justamente em virtude deste contexto que o presente trabalho se propõe a analisar o tema da difusão de normas, aproveitando-se de recursos metodológicos que consistem em pesquisa bibliográfica, estudo de caso e pesquisa documental relacionada ao caso.

Com relação à pesquisa bibliográfica, embora traga a visão de diferentes autores que se debruçam sobre o tema da difusão, o presente trabalho se apoia majoritariamente no livro da autora Anu Bradford, publicado em 2020, e denominado "O Efeito Bruxelas: como a União Europeia governa o mundo"[1]. Conforme explicado mais detalhadamente nos próximos capítulos, o "Efeito Bruxelas" caracteriza a habilidade de a UE em penetrar a vida de outras localidades a partir da exportação de normas facilitada por mercados, empresas privadas e dinâmicas de influência. Nesse sentido, é um material rico para revelar e interpretar as dinâmicas de difusão que permeiam a realidade e o caso concreto analisado neste estudo.

Por sua vez, o caso em estudo é o da difusão de regulamentações de proteção de dados pessoais desde a UE (a qual adotou, em 2016, o Regulamento Geral sobre a Proteção de Dados, apelidada adiante de RGPD) até o Brasil (o qual adotou, em 2018, a Lei Geral de Proteção de Dados Pessoais - LGPD). A escolha se deu por diferentes motivos, dentre eles as coincidências temporais entre as normas, as similaridades de suas previsões e a acessibilidade ao conteúdo do processo legislativo, mas especialmente por ser uma evidente representação do fenômeno da difusão.

Vale ainda pontuar a relevância deste trabalho que, sem a ambição de esgotar a possibilidade de dinâmicas de difusão serem analisadas sob outras lentes ou a revisão bibliográfica dos temas tratados, busca apontar de forma prática dinâmicas de influência, persuasão e negociação que permeiam o cotidiano da adoção de normas em um mundo globalizado e capitalista, bem como aproxima as literaturas do Direito e das Relações Internacionais com o objetivo de empregar uma visão holística e contextualizada sobre essas dinâmicas.

Para tanto, este trabalho se divide em três partes. A primeira, intitulado "A difusão internacional de normas em decorrência da necessidade de proteção de dados pessoais", traz o contexto social, econômico, jurídico que baseia a difusão de normas regulatórias acerca do tema da proteção de dados pessoais, revelando os motivos pelos quais o tema passou a ter relevância suficiente para se difundir.

A segunda parte, intitulada "O processo legislativo e o conteúdo normativo da LGPD como reflexo do RGPD: uma análise da difusão sob a perspectiva do 'Efeito Bruxelas'", analisa (i) o processo legislativo da LGPD, investigando narrativas,

[1] No original, "The Brussels Effect: How the European Union rules the world."

discursos e evidências encontradas em documentos oficiais do processo e em outros materiais disponíveis; e (ii) o conteúdo da lei, utilizando como ferramenta uma análise comparativa de suas disposições em relação ao teor normativo do RGPD. Assim, o capítulo evidencia os atores e demais marcos que potencialmente contribuíram para a adoção da LGPD como reflexo da normativa europeia (RGPD). Como revela o título do capítulo e antecipado anteriormente, a análise é em grande parte realizada sob a perspectiva do “Efeito Bruxelas” de Anu Bradford.

Já a terceira parte, nomeada “A difusão internacional de normas e a ruptura das visões tradicionais do sistema internacional”, debate – com atenção às evidências e marcos extraídos do capítulo anterior – os reflexos do processo de difusão de normas no sistema internacional e o potencial desafiador dessas implicações nas visões tradicionais desse sistema, interrelacionando perspectivas das Relações Internacionais e do Direito para uma compreensão holística e integrada.

2 A DIFUSÃO INTERNACIONAL DE NORMAS EM DECORRÊNCIA DA NECESSIDADE DE PROTEÇÃO DE DADOS PESSOAIS

O objetivo deste capítulo é trazer o contexto social, econômico, jurídico que baseia a difusão de normas regulatórias acerca do tema da proteção de dados pessoais, necessários à compreensão do tema.

Como explanado acima, o fenômeno da difusão é entendido como aquelas ações ou decisões tomadas localmente (seja em um país ou fórum específico) que repercutem globalmente, em outros níveis ou jurisdições. O fenômeno abrange, dentre outros tantos movimentos[2], a forma com as quais normas adotadas em determinado local difundem-se globalmente e influenciam outras jurisdições e, por vezes, o fenômeno recebe outros nomes, como “transferência” e “circulação” (OLIVEIRA; SARAIVA; SAKAI, 2020, p. 19).

Embora não se possa afirmar que a difusão de normas é um fenômeno recente, a globalização e a Era da Informação certamente são fatores intensificadores desse movimento, rompendo barreiras de segregação de pessoas, bens, serviços e tomadas de decisão em maior escala ou maior velocidade. A difusão de regulamentações de dados pessoais é um exemplo claro do resultado dessa intensificação.

O acesso e o uso de dados pessoais de indivíduos por empresas, governos e outras entidades de forma geral, para diferentes propósitos, tem levantado questionamentos e reflexões acerca da privacidade dos usuários de meios digitais. Diferentemente dos ambientes físicos privados em que somente os presentes seriam capazes de entender o que se passa no local, a utilização de espaços cibernéticos deixa pegadas que expõem os comportamentos e as preferências de seus usuários. Esses rastros são acessados por partidos políticos, governos e ente privados para diferentes finalidades, como cálculos estatísticos, vigilância, monitoramento ou simplesmente a oferta de produtos que melhor atendam às preferências de usuários (BECKER, 2016, p. 143).

É notável o papel exercido pelo setor privado, especialmente empresas dedicadas ao comércio de produtos e serviços eletronicamente, com relação a essa última finalidade. Há diferentes tipos de ferramentas de marketing que são

[2] Não são apenas normas jurídicas em seu sentido próprio que estão sujeitas ao fenômeno da difusão. Há, também, a difusão de políticas públicas (OLIVEIRA; SARAIVA; SAKAI, 2020, p. 19), boas práticas (NEWMAN; BACH, 2014, p. 431), revoluções e conflitos (BRAITHWAITE; JEONG, 2017, p. 1).

empregadas por esses atores e consistem na coleta de dados de usuários, análise organizada e apropriação dos resultados obtidos para emprego das estratégias relevantes a fim de impulsionar vendas, gerar interações e fidelização, dentre outros objetivos, propiciando uma interação direta entre empresa e potencial consumidor (CLARKE, 1990, 2.2 e 3.2; CANAVILLAS; CURRY; WAHLSTER, 2016, p. 3).

O Estado também tem um papel relevante nessa coleta e uso de dados pessoais para outras finalidades, tal como o uso de aplicações de geolocalização que acessam dados de rastreamento dos telefones móveis de indivíduos e, portanto, permitem a observação de deslocamentos com a finalidade de monitorar o surto da COVID-19 e as zonas vulneráveis (DATAPRIVACYBR, 2020).

Embora o objetivo dessas ferramentas pareça ser, e por vezes de fato são, o de propiciar ao usuário uma melhor experiência e uma solução customizada para atender ao seu perfil, há impactos mais sensíveis na coleta e rastreio de dados e comportamentos de indivíduos. Ainda que os dados coletados a partir dessas ferramentas não sejam necessariamente confidenciais (gênero, data de nascimento, nome e estado civil são, de forma geral, informações públicas ou ao menos à disposição do Estado), a forma com que eles são utilizados permite a empresas e governos que estes tomem decisões por seus usuários, ao mesmo tempo em que negam a esses indivíduos a possibilidade de participarem ativamente dessa decisão (SOLOVE, 2007, p. 756).

O tratamento de dados pessoais acaba por impactar também as oportunidades, modos e opções de vida dos indivíduos, não se tratando tanto de proibir ou não esse uso por entes privados, mas sim do direito de os indivíduos controlarem e aceitarem as condições de exposição e uso de suas informações (ROSEN, 2000, p. 35).

Soma-se à complexidade das condições de exposição e uso dos dados pessoais de indivíduos o fato de que referidas informações são armazenadas em datacenters dispostos ao redor do mundo, estando sujeitas, portanto, a um fluxo internacional de informações e normas aplicadas por diferentes ordenamentos jurídicos. Ainda que uma transação comercial ou determinada plataforma esteja restrita a um único território, as diversas relações que circundam àquela atividade podem envolver a transferência internacional de dados pessoais (como, por exemplo, o uso, por um usuário brasileiro, de nuvens para armazenamento de informações cujos servidores estejam fisicamente posicionados na Ásia).

A coleta, tratamento e circulação de dados pessoais de determinado indivíduo, assim, impactam sua privacidade. Abre-se aqui um parêntesis para esclarecer que o direito à privacidade integra os direitos da personalidade e está amparado por diferentes diplomas legais de caráter internacional, como a Declaração Universal dos Direitos do Homem de 1948 (ONU, 1948, art. 12) e a Declaração Americana dos Direitos e Deveres do Homem de 1948 (OEA, 1948, art. 5º), e nacional, como a Constituição Federal de 1988 (BRASIL, 1988, art. 5º, inciso X) e o Código Civil Brasileiro de 2002 (BRASIL, 2002, art. 21).

Assim como outros direitos fundamentais, a literatura entende que a proteção ao direito à privacidade deve ser assegurada pelo Estado tanto por meio de uma atuação negativa, abstendo-se este de atos que possam invadir a liberdade individual dos cidadãos, quanto positiva, por meio da implementação de ações que busquem assegurar a manutenção dessa liberdade (MONTEIRO, 2007, p. 28).

De acordo com Rosen (2000, p. 34), até o século XVIII as noções de direito à propriedade privada eram, de modo geral, suficientes para assegurar a privacidade dos indivíduos. O autor traduz essa circunstância exemplificando a situação de que "se você quisesse ler meu diário, você teria que invadir minha casa, e se você invadisse minha casa, eu poderia processá-lo por invasão." [3] (2000, p. 34, tradução livre). Atualmente, porém, os reflexos das ações e intelectualidade dos indivíduos deixou de limitar-se a espaços físicos, passando a integrar ambientes cibernéticos que por natureza são abstratos, descentralizados e integrados por diferentes atores, dificultando o controle ou a tomada de decisão a respeito dos dados pessoais pelos próprios donos dessas informações.

De acordo com a autora Patricia Peck Pinheiro (2021, p. 77), o crescente risco à segurança da informação exige regulamentação para que se pudesse conferir "garantias mínimas para os titulares bem como alguns novos direitos que permitissem o seu empoderamento no tocante a um maior poder de decisão sobre o uso de suas informações".

Esse efeito é mais uma representação da globalização que repercute em contextos sociais, econômicos, culturais e políticos, revelando a participação de outros atores além dos Estados. Dentre esses atores estão empresas com atuação transnacional que levantam indagações acerca dos limites e responsabilidades destas

[3] No original, "if you wanted to read my diary, you had to break into my house, and if you broke into my house, I could sue you for trespass."

quanto aos direitos humanos de forma geral (PIOVESAN; GONZAGA; 2019, p. 12; LESSA; REIS, 2017, p. 26-27), inclusive o direito à privacidade que se busca assegurar por meio da proteção aos dados pessoais.

De acordo com Ana Cláudia Ruy Cardia (2014, p. 40), a atuação das empresas transnacionais confronta o cenário tradicional em que os Estados eram capazes de isoladamente controlar suas próprias economias, de modo que a relevância do setor empresarial na sociedade internacional deve ser reconhecida para que referidos Estados não deixem de encarar e acompanhar a realidade econômica que se apresenta atualmente.

Diante desses e outros dilemas é que surge a necessidade de regulamentação quanto à coleta, tratamento e uso de dados pessoais, movimento este que vem ocorrendo globalmente.

A partir dos anos 2000, já é possível observar, em diferentes ordenamentos jurídicos, o surgimento de normas acerca do uso da Internet que atacam a proteção da privacidade, mas que possuem caráter predominantemente principiológico ou de pouco alcance para resolução de um problema de escala mundial (i.e., no Brasil, o Marco Civil da Internet; na UE, a Diretiva de Proteção de Dados Pessoais de 1995, que precedeu o RGPD) (TOMASEVICIUS, 2016, p. 276).

Contudo, o surgimento de regulamentações específicas quanto ao tratamento de dados pessoais intensificou-se em meio à aprovação do RGPD pela UE, em 2016 (UE, 2016). A partir de então, Brasil, Estados Unidos e Japão são apenas alguns dos países que estabeleceram novas regulamentações para atender às demandas específicas do compartilhamento de dados pessoais, por meio da LGPD (BRASIL, 2018), a Lei da Califórnia de Privacidade do Consumidor de 2018 (EUA, 2018) – dentre as demais normas dos Estados Unidos que são promulgadas em nível federal e estadual e tratam da proteção de dados pessoais de forma mais específica, aplicada a determinados setores da economia ou sociedade, como a Lei Contra Hackeamento e de Aprimoramento à Segurança da Informação Eletrônica de Nova Iorque (EUA, 2020) - e Emenda à Lei sobre a Proteção de Informações Pessoais de 2016 (JAPÃO, 2016).

Embora essas legislações estejam à primeira vista espacialmente distantes, percebe-se que há um movimento global relacionado à proteção de dados pessoais que está submetido a um movimento constituído por debates, diretrizes e regulamentações tratadas internacionalmente.

Nesse movimento, a UE atuou como protagonista e propulsora de um “efeito dominó” na difusão de regulamentações de proteção de dados pessoais (CHOW; LIMA, 2021, p. 306) – efeito este que se reflete em âmbito local, por meio da promulgação de norma que regula o tratamento de dados pessoais no Brasil.

Diante desse cenário, passa-se a um estudo de caso, por meio da análise da difusão da regulamentação de proteção de dados pessoais adotada pela UE - o RGPD - ao Brasil, por meio da promulgação da LGPD.

3 O PROCESSO LEGISLATIVO E O CONTEÚDO NORMATIVO DA LGPD COMO REFLEXO DO RGPD: UMA ANÁLISE DA DIFUSÃO SOB A PERSPECTIVA DO "EFEITO BRUXELAS"

O contínuo fluxo de informações que viajam por meio da internet independentemente de limites territoriais e fronteiras geográficas é um significativo elemento da sociedade global do século XXI. Esse fluxo está permeado de diferentes dinâmicas entre empresas, instituições, governos e indivíduos que têm seus dados pessoais coletados e tratados transnacionalmente para diferentes finalidades, como tratado no capítulo anterior.

Com o uso da internet em praticamente todos os campos da vida atual, a transferência internacional de dados pessoais está no cotidiano dos negócios, governos e das interações sociais. Na prática, ela ocorre a partir da contratação de ferramentas estrangeiras para diversas atividades (como, por exemplo, serviços em nuvem ou ferramentas de marketing para maior alcance de anúncios e publicidade), compartilhamento de base de dados entre empresas do mesmo grupo econômico, armazenamento de dados em servidores frequentemente localizados no exterior, aquisição de produtos em sites estrangeiros, interações em redes sociais entre usuários de diferentes países, entre outras formas (ROSEN, 2000, p. 32-38; BECKER, 2016, p. 143-145).

Assim, o fluxo internacional de dados pessoais tornou-se mais frequente e mais desterritorializado, fazendo emergir preocupações e "trade-offs" sob diferentes perspectivas.

Por um lado, a difusão de dados pessoais sem ciência ou transparência pode ser um transtorno para aquele que são incomodados por telemarketings ofertando serviços que não são de seu interesse, tem seus comportamentos mapeados em perfis que limitam suas interações online ou até mesmo sofrem prejuízos financeiros e morais a partir da violação de contas bancárias, clonagens e outros ilícitos facilitados pelo acesso indiscriminado de suas informações.

Por outro lado, dados pessoais são verdadeiros ativos que podem ser essenciais para a consecução de atividades por empresas e governos ou, quando não imprescindíveis, ao menos conferem vantagens competitivas e podem servir de fontes de estudo e inovação. Indivíduos também se beneficiam quando obtêm ofertas customizadas, possuem maiores mecanismos de consulta de melhores preços e

usufruem de políticas públicas adaptadas à sua realidade que possibilitados a partir do tratamento de seus dados pessoais.

Naturalmente, o surgimento de regulamentações de proteção de dados pessoais acabou por impactar não apenas indivíduos a respeito dos quais os dados se referem, mas também entidades privadas e públicas que se sujeitam a essas normas, em diferentes formatos e graus de severidade, a depender do tipo de dado e da jurisdição.

Embora a UE não seja a única jurisdição a adotar uma regulamentação de proteção de dados pessoais - Estados Unidos e Japão, dentre outros países, já possuíam normativas a respeito, conforme exposto acima -, ela teve um papel de protagonismo na difusão dessas normativas mundialmente, inclusive para o Brasil, a partir da promulgação do RGPD em 2016.

O próprio teor do RGPD já pode ser especulado como um dos motivos pelos quais a norma foi essencial para a difusão de regulamentações da mesma natureza. O RGPD tem um caráter bastante protetivo quanto ao tratamento de dados pessoais, já que direito à privacidade é um direito fundamental sob a perspectiva da Carta dos Direitos Fundamentais da UE (UE, 2000, art. 7º e 8º)[4], diploma legal que reúne formalmente em um único documento os direitos humanos tutelados pela UE e os países que a integram. Há, assim, uma base legal que suporta a intenção de conferir aos indivíduos sujeitos à RGPD o controle e autodeterminação quanto aos seus dados pessoais (BRADFORD, 2020, p. 154).

Essa extensão é reforçada pelo fato de que a aplicabilidade do RGPD não se restringe às suas fronteiras (CHOW, LIMA, 2021, p. 304). De acordo com a norma, todas as empresas que coletam, armazenam e processam dados pessoais de residentes da UE devem obedecer a normativa. Isso torna a norma bastante abrangente ao lembrarmos que, como tratado anteriormente, dados pessoais são frequentemente processados ou armazenados de forma descentralizada, por ferramentas estrangeiras ou servidores presentes em diferentes países (UE, 2016, art.

[4] "Artigo 7º. Respeito pela vida privada e familiar Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações."
"Artigo 8.o Proteção de dados pessoais 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente."

44)[5]. Caso a empresa que trata os dados pessoais não esteja em um país capaz de assegurar um nível de proteção equivalente ao da UE (seja por força de lei ou por meio da assunção de compromissos contratuais específicos de proteção), o tratamento de dados pessoais é vedado (UE, 2016, art. 44).

A presença de previsões normativas que estabelecem a aplicabilidade extraterritorial do RGPD não pode ser subestimada. Regulamentações antecedentes, como a Diretiva de Proteção de Dados de 1995, da própria UE, e as regulamentações dos EUA, não estabelecem condições aplicáveis à transferência internacional de dados pessoais, gerando adesão de países terceiros para adaptação.

Em junho de 2021, o Japão também promulgou uma alteração à sua lei de privacidade e proteção de dados, o "Act on the Protection of Personal Information" - APPI (JAPÃO, 2021), com novas exigências e a previsão de que negócios não precisam ser operados no Japão para que estejam sujeitos à APPI, mas apenas tratar dados de pessoas localizadas no Japão, assim como o RGPD. A APPI, semelhantemente à RGPD, também passou a diferenciar dados pessoais de dados pessoais sensíveis, sendo este último dados que podem de alguma forma gerar discriminação e, portanto, são merecedores de maior proteção. Essas duas condições também estão presentes na LGPD e normativas de outros países promulgadas após o RGPD.

Esses fatores sinalizam a atuação da UE como *agenda-setter* no tema de proteção de dados pessoais (CHOW; LIMA, 2021, p. 304), ao promover determinado tema dentre a comunidade internacional em detrimento de outros assuntos, como uma ferramenta de garantir e estender poder com relação aos demais atores (LIVINGSTON, 1992, p. 313).

Essa dinâmica de influência da UE é estudada por Anu Bradford (2020, p. 15), que chama de "Efeito Bruxelas" a habilidade da UE de promulgar regulamentações que moldam o sistema econômico global e o poder de regulamentar mercados unilateralmente (isto é, sem que seja por meio de organizações internacionais ou

[5] "Artigo 44.o Princípio geral das transferências Qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional só é realizada se, sem prejuízo das outras disposições do presente regulamento, as condições estabelecidas no presente capítulo forem respeitadas pelo responsável pelo tratamento e pelo subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional. Todas as disposições do presente capítulo são aplicadas de forma a assegurar que não é comprometido o nível de proteção das pessoas singulares garantido pelo presente regulamento"

mediante cooperação com outros países). Desse modo, regulamentações que, a princípio, se limitam à sua ordem jurídica acabam por penetrar a vida econômica de outras localidades, sendo exportadas internacionalmente a partir de uma influência facilitada por mercados e empresas privadas.

De acordo com a autora, a expansão das regulamentações europeias para além de suas fronteiras podem ser analisadas sob duas perspectivas: a perspectiva “de facto” e a perspectiva “de jure”. Enquanto a perspectiva “de facto” observa o modo com que empresas e outros autores convergem à adoção da regulamentação europeia, a perspectiva “de jure” expõe como governos não pertencentes à UE adotam domesticamente regulamentações similares (BRADFORD, 2020, p. 19).

Em sua obra, Anu Bradford (2020, p. 152) se dedica a explorar a influência regulatória da UE em diversas áreas, dentre elas a área da economia digital, e sinaliza que poucas normas impactaram tanto empresas digitais globais quanto o RGPD e o Código de Conduta Contra o Discurso de Ódio da Comissão da UE (normativa voluntária e elaborada com a participação de gigantes da tecnologia - Facebook, Twitter, Youtube e Microsoft).

No passado, a Diretiva Europeia de Proteção de Dados de 1995 (UE, 1995) era suficiente para cobrir o objetivo de integrar os fluxos de dados pessoais somente entre o mercado europeu. Contudo, com a globalização do processamento de dados pessoais e a importância da transferência internacional de dados para além do mercado europeu, a UE encontrou motivação para estabelecer padrões e buscar compliance com os requisitos e exigências de proteção que entende adequados antes que outros atores o fizessem. Paralelamente, consumidores e parcela da sociedade civil pressionavam para a adoção de medidas de proteção de dados mais restritivas, enquanto empresas e governos estrangeiros (em especial os Estados Unidos) resistiram em prol de uma mitigação de custos na adoção de uma nova regulamentação (BRADFORD, 2020, p. 137).

Em que pese esses embates, o RGPD foi promulgado e muitas empresas estrangeiras estão ajustando suas práticas de negócios para refletir as normas europeias, enquanto muitas jurisdições adotam modelos semelhantes ou compatíveis com o RGPD internamente. Esse movimento é reflexo da crescente relevância do setor empresarial no cenário internacional que permitiria uma análise de quais normas internacionais o setor empresarial de determinada localização quer seguir, em lugar

de analisar a quais normas locais estão sujeitos, colocando o setor em um papel de protagonismo (ALVAREZ, 2011, p. 32).

O exemplo que nos interessa o Brasil, com a promulgação da LGPD, cujo movimento e influência do RGPD é analisada nos parágrafos seguintes a partir da perspectiva “de facto” e “de jure” da teoria do “Efeito Bruxelas” de Anu Bradford.

3.1 O processo legislativo da LGPD e a análise da influência do RGPD sob a perspectiva “de facto” de Anu Bradford

3.1.1 O processo legislativo

O histórico do processo legislativo da LGPD remonta ao de 2010, ano em que o Ministério da Justiça brasileiro realizou a abertura da 1ª consulta pública sobre o anteprojeto de lei de dados pessoais, tendo contado com a participação de diferentes setores da sociedade. Em 2012, é apresentado na Câmara dos Deputados o PL nº 4060/2012, pelo Deputado Milton Monti - projeto que deu origem à Lei nº 13.709/2018, a LGPD - cujo teor de 25 artigos espalhados em 6 páginas era muito mais simples e menos específico que o texto final aprovado, mas que em sua justificativa já trazia evidências de participação do setor da Indústria da Comunicação (BRASIL, 2012).

Após apensação, desapensação e arquivamentos comuns aos processos legislativos[6], o PL é desarquivado em 2015 e o ritmo de sua tramitação intensifica-se, contando com a participação do setor empresarial e a motivação de acompanhar as legislações estrangeiras, em especial a UE, no tema. O quadro abaixo sistematiza e exibe os principais marcos da tramitação do projeto (BRASIL, 2012), dentre os quais aqueles que evidenciam a participação do setor empresarial e o acompanhamento das normas internacionais (na coluna esquerda, estão escritos quais andamentos da tramitação, enquanto na coluna direita está descrito o teor dos referidos andamentos):

Quadro 1 – Análise de documentos oficiais do processo legislativo da LGPD

Andamento	Trecho extraído dos documentos

[6] Importante esclarecer que, em determinados momentos, o PL correu em apensado com outros projetos, assim como recebeu outras numerações em virtude de mudança de casas legislativas, por exemplo. Contudo, para fins didáticos, citar-se-á tão somente o PL nº 4060/2012, versão original que resultou na LGPD.

06/05/2015 - Apresentação do Requerimento nº 44/2015, pelo Deputado Sergio Zveiter (PSD-RJ), aprovado em 20/05/2015	"Requer sejam convidados representantes da **Associação Brasileira de Agências de Publicidade (ABAP), Associação Brasileira de Marketing Direto (ABEMD) e da Associação Brasileira das Empresas de Rádio e Televisão (ABERT)**, para, em Audiência Pública no âmbito da Comissão de Ciência e Tecnologia, Comunicação e Informática, discutir os aspectos da Lei de Proteção de Dados Pessoais. (...) Justificação. (...) Essa situação leva, naturalmente, à necessária regulação do conteúdo, uso e tratamento desses dados, elaborando um ordenamento jurídico mais adequado à realidade atual. **Cabe ressaltar que o Brasil encontra-se atrasado em relação a outras nações que já possuem leis específicas para proteção de dados**. Nossa realidade resume-se ao habeas data e alguns artigos do CDC que tratam da manutenção de bases de dados e cadastro de consumidores, ou seja, não existe de fato nada que possa limitar o uso não autorizado de informações pessoais. Dentro dessa realidade se faz necessário estabelecer normas legais para disciplinar tais relações, especialmente para dar proteção à individualidade e a privacidade das pessoas."
17/09/2015 - Apresentação do Requerimento de Audiência Pública nº 99/2015, apresentado pelo Deputado Sergio Zveiter (PSD-RJ), aprovado em 23/09/2015	"Requer sejam convidados representantes da Secretaria Nacional do Consumidor - Ministério da Justiça (Senacon/MJ), da **Associação Brasileira de Emissoras de Rádio e Televisão (Abert)**, do Instituto Brasiliense de Direito Público (IDP), e o professor Pablo Ortellado - Professor da Universidade de São Paulo (USP), para aprofundar a discussão acerca dos aspectos da Lei de Proteção de Dados Pessoais, iniciada em audiência pública anteriormente realizada no âmbito da Comissão de Ciência e Tecnologia, Comunicação e Informática."
04/05/2016 - Apresentação do Parecer do Relator nº 1 CCTCI, pelo Deputado Sóstenes Cavalcante (DEM-RJ)	"De fato, o Brasil demanda uma legislação sobre a matéria, em face do crescimento desse tipo de atividade e da comercialização ilegal desse tipo de informação. Além disso, no ano de 2013 veio a público relato de que as principais empresas de Internet sediadas nos Estados Unidos da América, entre elas o Google e o Facebook, violam a privacidade de seus usuários, franqueando o acesso a esses dados à NSA, a agência de segurança americana. O Google, especificamente, admitiu que os usuários de seu serviço de e-mail, o Gmail, não têm "expectativa razoável" de que suas mensagens não sejam violadas, e, além disso, afirmou em processo judicial, que corre em corte norte-americana, que "todos os usuários de e-mail devem necessariamente esperar que seus e-mails sejam sujeitos a processamento automático". Esse contexto, portanto, deixa evidente a premência de uma legislação como a que analisamos. **Os termos do projeto estão alinhados com legislações estrangeiras, entre as quais destacamos a Diretiva 95/46/CE da União Europeia, que se aplica aos dados tratados por meios automatizados**."
17/05/2016 - Apresentação do Requerimento de Audiência Pública nº 150/2016, pelo Deputado Sibá Machado (PT-AC), aprovado em 01/06/2016	"O usuário teria o direito de proibir o tratamento de seus dados pessoais, porém se houver previsão contratual em sentido contrário, o usuário não terá esse direito. **Em outras palavras, basta que nos termos de uso do Facebook, por exemplo, haja proibição de o usuário solicitar o bloqueio do tratamento de seus dados pessoais, para que a lei não tenha eficácia (art. 13)**. O PL 4060/2012 autoriza a comercialização dos dados pessoais e não estabelecer pesos e contrapesos, tampouco penas pela violação (art. 14). O PL 4060/2012 propõe a criação de Conselhos de Autorregulamentação do setor, o que nos parece tendencioso e pouco protetivo dos dados pessoais de seus

	titulares (art. 23). Em sendo assim, faz-se necessária a realização de audiência pública para que esta Casa possa receber subsídios para a mais equilibrada legislação sobre o assunto.”
09/08/2016 - Plenário - Requerimento de Redistribuição nº 5.017/2016 pelo Deputado Orlando Silva (PCdoB-SP), aprovado em 18/08/2016	“O Brasil não possui uma legislação ligada à proteção de dados pessoais, um dos pilares do Marco Civil da Internet (lei 12.965/2014). Atualmente, **mais de 100 países já possuem leis de proteção de dados pessoais, nesse contexto a regulamentação de proteção de dados pessoais é um dos desafios da atualidade para o país**. (...) Outrossim, **busca-se na proposição, a obtenção de benefícios econômicos e sociais potencializados pela tecnologia da informação, ao criar no país uma arquitetura regulatória capaz de proteger os dados pessoais**. Diante do exposto, uma vez que o referido Projeto **interfere na ordem econômica nacional e afeta diretamente as relações econômicas internacionais, a ordem econômica nacional e comércio exterior; políticas de importação e exportação em geral (Art. 32, VI, “a”, “b” e “e”, do Regimento Interno), requeiro a revisão do despacho de distribuição a fim de incluir a Comissão de Desenvolvimento Econômico, Indústria, Comércio e Serviços no rol das Comissões Permanentes** que devem se manifestar quanto ao mérito da proposição e concomitante a criação de comissão especial conforme Art. 34, II.”
09/11/2016 - Apresentação do Requerimento nº 1/2016, pelo Deputado André Figueiredo (PDT-CE), aprovado em 22/11/2016	“Requer autorização para realizar missão oficial, composta de membros desta Comissão Especial do PL 4060/12 - Tratamento e Proteção de Dados Pessoais Especial e servidores do seu quadro técnico ao **Vale do Silício na Califórnia, para participar do Fórum de Privacidade e Proteção de Dados Pessoais**, que ocorrerá do dia 30 de novembro ao dia 2 de dezembro.”
21/11/2016 - Apresentação do Requerimento de Audiência Pública nº 3/2016, pelo Deputado Orlando Silva (PCdoB-SP), aprovado na mesma data	“Requer a realização de audiência pública para debater o tema: 'conceitos fundamentais sobre dados pessoais', com a as seguintes autoridades: Rafael Zanatta - Instituto Brasileiro de Defesa do Consumidor; Sergio Paulo Gallindo - **Presidente da Associação Brasileira de Empresas de Tecnologia da Informação e Comunicação - BRASSCOM**; Hartmut Richard Glase - Secretário Executivo do Comitê Gestor da Internet no Brasil/CG; e um Representante da Secretaria Nacional de Defesa do Consumidor do Ministério da Justiça.”
22/11/2016 - Apresentação do Requerimento nº 5/2016, pelo Deputado Thiago Peixoto (PSD-GO), aprovado na mesma data	“Requeiro a Vossa Excelência, nos termos regimentais, ouvido o Plenário, **que seja convidado o Representante da Seção Americana do Conselho Empresarial Brasil-EUA,** com o intuito de debater aspectos atinentes ao PL 4060/2012. (...) JUSTIFICATIVA (...) A Seção Americana do Conselho Empresarial Brasil-Estados Unidos enviou comentários à regulamentação do tratamento de dados pessoais. Nesse sentido, o comparecimento do representante contribuirá para o debate e esclarecimentos sobre o tema em questão.”
25/11/2016 - Apresentação do Requerimento de Audiência Pública nº 8/2016, pelo Deputado Roberto Alves (PRB-SP),	“Requer a realização de Audiência Pública com a presença do Sr. Antônio Guerreiro - representante da **Abratel (Associação Brasileira de Rádio e Televisão)**.”

aprovado em 14/12/2016	
06/12/2016 - Apresentação do Requerimento nº 9/2016, pelo Deputado Thiago Peixoto (PSD-GO), aprovado em 14/12/2016	"Requer a realização de audiência pública com os seguintes convidados: Eduardo Fumer Parajo - **Presidente da ABRANET; Francisco Camargo - Presidente da ABES; Frederico Meinberg - Professor do IBDDIG; Elias Sfeir - Presidente da ANBC**."
03/04/2017 - Apresentação do Requerimento nº 13/2017, pelo Deputado Orlando Silva (PCdoB-SP), aprovado em 05/04/2017	"Requer a realização de audiência pública na comissão especial destinada a proferir parecer ao PL nº 4060 de 2012 com a presença dos seguintes convidados: Bruno Magrani do **Facebook**; Leonardo Bessa do Instituto Brasileiro de Política e Direito do Consumidor - BRASILCON; Denny Antonialli do InternetLab; Cintia Rosa Pereira Lima da Faculdade de Direito USP; Pedro Mizukami do CTS/FGV; Guilherme Varella, Pesquisador; Virgílio Almeida da Faculdade de Harvard; Fabricio Solagna do Centro de Estudos Barão de Itararé; e Representantes do Ministério Público do Distrito Federal e Territórios - MPDFT, da Open Knowledge Foundation, **do Mozilla, da Empresa Brasileira de Comunicação - EBC**; do Fórum Nacional pela Democratização da Comunicação - FNDC; **Motion Pictures Association - América Latina; da UOL/Folha; da Associação Brasileira da Indústria Elétrica e Eletrônica - Abinee; e do Creative Commons.**"
11/05/2017 - Apresentação do Requerimento nº 14/2017, pelo Deputado Thiago Peixoto (PSD-GO), aprovado em 12/07/2017	"Requer a realização de Audiência Pública desta Comissão Especial com a Sra. Cris Camargo, Diretora Executiva da **Interactive Advertising Bureau - IAB Brasil**"
24/05/2018 - Comissão Especial destinada a proferir parecer ao PL nº 4060/2012 - Apresentação do Parecer do Relator nº 1 PL406012, pelo Deputado Orlando Silva (PCdoB-SP)	"**Importante pontuar que as propostas se inserem em um contexto mundial, portanto, maior, em que legislações nacionais são introduzidas em cada país, de forma a tratar da questão dos dados pessoais e garantir a proteção das pessoas de maneira harmônica**. Ao mesmo tempo, a construção de um arcabouço similar entre os países gera um ambiente propício aos negócios, principalmente globais, oriundos do manuseio de dados. De fato, a Mensagem do Poder Executivo, ao PL no 5.276/16, ressalta que a proposta é fruto da Resolução da ONU, de 25 de novembro de 2013, sobre "Direito à Privacidade na Era Digital", e que "109 países possuem normas nesse sentido e mais de 90 destes têm uma autoridade pública específica especializada no tema". **Nesta contextualização internacional é importante observar que a Diretiva Europeia, extensamente detalhada e que possui 99 artigos e 173 notas explicativas, não permite a transferência internacional de dados para países que não possuam legislação que garanta a mesma proteção dada pela Lei Europeia**. (...) Esse ponto, de a legislação do país estar de acordo com a legislação europeia, **é extremamente pertinente neste julgamento, pois indica, como questão de fundo, a atratividade comercial do setor de TIC (Tecnologia da Informação e das Comunicações) dos países. Em tempos de computação em nuvem, um país que atenda à legislação europeia possui condições de atrair processamento de dados**

	daquele bloco. E atrair o tratamento de dados implica não só a possibilidade de instalação de data centers, mas das próprias empresas de TIC, incluindo as gigantes ponto com. Por isso, a **necessidade de o Brasil possuir, sem abrir mão de suas especificidades e soberania, uma legislação harmônica com o mundo e com os principais blocos organizados, como a União Europeia**. Devido a esses dois aspectos, o da necessidade da promoção da proteção da pessoa humana e o do desenvolvimento e da integração do setor de TIC como ferramenta de desenvolvimento econômico para o País, somos, no mérito, pela aprovação das matérias."
29/06/2018 – Apresentação de relatório favorável ao Projeto de Lei da Câmara nº 53/2018, pelo senador Ricardo Ferraço	"A despeito do contexto de crise econômica, **é seguro afirmar que o País tem perdido oportunidades valiosas de investimento financeiro internacional em razão do isolamento jurídico em que se encontra por não dispor de uma lei geral e nacional de proteção de dados pessoais (LGPD)**. O dado pessoal é hoje insumo principal da atividade econômica em todos os setores possíveis da sociedade. Um regime de proteção de dados, portanto, quando eficaz e plenamente vigente, impulsiona o surgimento de ecossistema de dados, no qual todos os setores da sociedade, inclusive o cidadão, são diretamente beneficiados. Ao longo desta relatoria, ouvimos diversas empresas, associações e representantes da sociedade civil, que trouxeram contribuições impressionantes sobre como a utilização responsável de dados pessoais pode expandir negócios e impulsionar a economia."

Fonte: BRASIL, 2012. Grifos da autora.

Para além dos registros documentais oficiais que integram o processo legislativo, há outras evidências da atuação do setor privado na aprovação da LGPD, bem como do papel de impulsionador da EU, que são encontrados em posicionamentos, entrevistas de indivíduos que atuaram durante o processo e notícias.

Por exemplo, Sergio Paulo Gallindo, Diretor Executivo da Brasscom, ressalta, em entrevista concedida, que, em 2016, referida associação encabeçou a elaboração de um manifesto em defesa do PL, indicando todos os pontos do texto que eram considerados essenciais para seus associados e com o objetivo de que o manifesto tivesse a capacidade de obter apoio de outras associações (GALLINDO, 2019, item 11). Ao fim, o movimento resultou no Manifesto sobre a Futura Lei de Proteção de Dados Pessoais datado de setembro de 2016 (ABRANET, 2016), o qual encontra-se transcrito no Anexo A deste trabalho, com o apoio e subscrição de diversas associações representativas do setor privado (ABEMD, ABES, ABRANET, ANBC, ASSESPRO, além da própria BRASSCOM), tendo passado a ser, nas palavras de Sergio Paulo Gallindo, "um marco de referência na Câmara dos Deputados em relação à tramitação", de modo que "a discussão girou sempre em torno desses pontos

basilares daquilo que nós entendíamos que era essencial na lei" (GALLINDO, 2019, item 11).

Já em 13 de julho de 2018, surgiu outro manifesto, desta vez o Manifesto pela Aprovação da Lei de Proteção de Dados Pessoais (BRASSCOM, 2018), o qual encontra-se disponível para consulta no Anexo B deste trabalho, cujo objetivo era demonstrar apoio à apreciação e aprovação do PL nº 53/2018 pelo Senado Federal. O Manifesto foi apresentado ao Senado Federal com 80 subscrições, dentre elas entidades representativas, comunidade acadêmica, indivíduos e organizações privadas, tratando-se de verdadeira coalização multissetorial (DATAPRIVACYBR, item 19). O Manifesto contou com a subscrição de diversas associações representativas de entes do setor privado, quais sejam: ABA, ABAP, ABCD, ABEMD, ABERT, ABES, ABDOH, ABRANET, ABRARC, ABRASEM, ABRATEL, ANJ, ANER, ANID, APP, ARPEN-Brasil, AsBraAp, Assespro, Brasscom, CACB, Camara-e.net, CAMP, FecomercioSP, Fenainfo, FENAPRO, Grupo de Mídia São Paulo, IAB Brasil, MBC, P&D Brasil, SEINESP e SEPROSP.

Este segundo Manifesto deixa claro em seu teor que a necessidade de o Brasil acompanhar o movimento de regramentos de proteção de dados pessoais por outros países, estar inserido internacionalmente do país, bem como atrair investimentos e negócios, são justificativas e motivações para a apreciação e adoção da lei, conforme descrito a seguir:

> Vários países já contam com regramentos de proteção de dados pessoais, endereçando os desafios da transformação social e da econômica decorrente do avanço da tecnologia digital, em reconhecimento ao enorme potencial de desenvolvimento bem-estar derivado da geração, coleta e tratamento de expressiva quantidade de dados. Uma lei de proteção de dados clara e principiológica, que equilibre a posição central do indivíduo com o dinamismo econômico de um país criativo e inclinado à inovação, como o Brasil, é essencial para catalisar competitividade.
> (...)
> O Senado tem oportunidade ímpar de conferir protagonismo ao Brasil, em termos de legislação de dados, passo fundamental para a inserção do País em foros internacionais bem como, de proporcionar um ambiente de negócios seguro que potencialize a atração e materialização de investimentos na ordem de R$ 250 bilhões (Brasscom e Frost & Sullivam) em tecnologias de transformação digital até 2021. O PLC nº 53/2018, ora sob a análise do Senado, é considerado pelos signatários deste manifesto, um texto que está em sintonia com as melhores práticas internacionais, equilibrando a garantia dos direitos individuais com a indução de novos modelos de negócios intensivos em dados. (BRASSCOM, 2018, p. 1)

Como contraponto, entidades que, em determinados momentos do processo legislativo, possuíam posições antagônicas ao setor privado destacam a existência de “ampla coalizão de empresas do setor de tecnologia e publicidade” (IDEC, 2016, p. 2) e qualificam que “o lobby do setor privado para flexibilizar o controle é bem forte” (TORRES, 2019), tendo publicamente combatido esses posicionamentos.

Em entrevista, Rafael Zanatta, ex-líder do programa de direitos digitais do IDEC, destaca que a própria origem da LGPD, refletida no PL 4060/2012, já evidenciava a participação do setor privado, conforme a seguir:

> (...) o [PL] 4060 é fruto de uma série de conferências e reuniões que as empresas de marketing organizam e as associações de marketing puxam essa iniciativa de ter um primeiro projeto, que é o 4060 do Milton Monti. (...) Então claramente o setor [privado] preparou o PL, municiou o parlamentar e ele apresentou. Evidentemente as empresas de tecnologia de grande porte, como o Facebook e o Google, estavam acompanhando desde o começo isso. (ZANATTA, item 7).

Também em entrevista concedida, Andriei Gutierrez, ex-diretor de relações governamentais e assuntos regulatórios da IBM, contextualiza o debate em torno do processo legislativo da LGPD mencionando que, a princípio, a atuação do setor privado se deu mais com o envolvimento de empresas de tecnologia que enxergavam a importância da regulamentação em virtude do impacto econômico do tema e buscavam apoio de outros setores, já que o assunto era percebido como um tema de informática. De acordo com Gutierrez, o PL correu em meio a debates com as organizações da sociedade civil que demarcavam a ausência de um consenso desde 2010, quando ocorreu a 1ª consulta pública acerca da proteção de dados pessoais (GUTIERREZ, 2020).

Gutierrez ainda menciona que um consenso foi encontrado quando o texto tramitava na Câmara dos Deputados, após negociações e concessões que partiram tanto da sociedade civil que defendia uma lei mais protetiva, quanto da sociedade civil mais alinhada ao setor privado (cuja atenção era não prejudicar a inovação) (GUTIERREZ, 2020).

Em maio de 2018, aproximadamente seis anos após a apresentação inicial do PL 4060/2012, houve a votação pela Câmara dos Deputados que decidiu pela aprovação do projeto, abrindo espaço para votação do projeto no Senado Federal.

Um fator cronológico interessante é o de que a votação na Câmara dos Deputados ocorreu 4 dias após a entrada em vigor do RGPD, a norma europeia de

proteção de dados pessoais (DATAPRIVACYBR, item 4 e item 16), tendo inclusive a própria UE passado a acompanhar a evolução do processo legislativo no Brasil (ALVES, 2019, item 4). Na perspectiva de Fabrício de Mata Alves, ex-assessor técnico no Senado Federal:

> (...) a entrada em vigor do RGPD foi outro fator muito relevante. Eu penso que mais em função da pressão que as grandes empresas, as big techs, que estavam acompanhando o projeto, acabaram entendendo que era melhor ter uma lei muito parecida com o RGPD no Brasil do que ter uma lei muito distante e você ter que lidar com mais uma regulação internacional diferenciada. Então as empresas começaram também a movimentar suas assessorias, suas consultorias políticas, para que o projeto voltasse a tramitar e dentro de um ambiente controlado. (ALVES, item 4).

Uma vez que o texto chegou ao Senado Federal para apreciação, “outros setores empresariais resolveram acordar”, nas palavras de Andriei Gutierrez, razão pela qual houve a montagem de uma coalizão com a participação ativa do setor empresarial (com liderança da BRASSCOM), da academia e da sociedade civil de forma geral para obter o sancionamento da LGPD de acordo com o texto cujo consenso foi obtido na instância inferior (GUTIERREZ, 2020; DATAPRIVACYBR, item 20).

Em agosto do mesmo ano, o PL foi sancionado pelo então Presidente Michel Temer, após aprovação e remessa pelo Senado Federal no mês anterior, sendo transformado na Lei Ordinária nº 13709/2018 - a LGPD.

Como expõe o quadro, relatos e evidências acima, na tramitação do PL há a recorrente presença dos argumentos de que o Brasil deveria adotar a normativa como forma de adequação, vez que estaria atrasado em comparação com as legislações de outros países que já possuíam diplomas visando à proteção de dados pessoais (dentre eles, a UE), reduzindo assim as chances de obtenção de investimentos financeiros internacionais, bem como precisaria de uma regulamentação harmônica com o RGPD, já que a normativa europeia não permite a transferência internacional de dados para países que não possuem o mesmo nível de segurança, o que, portanto, impactaria a atratividade econômica do setor de Tecnologia da Informação e das Comunicações brasileiro.

Na tramitação do PL, há também evidências de intensa participação do setor privado - por meio das entidades citadas no quadro acima e outras para além das mencionadas - seja por meio de uma representação direta, como é o caso do

Facebook e do Mozilla, seja por meio de associações representativas de diferentes segmentos, como a ABAP, a ABEMP e a BRASSCOM.

3.1.2 A perspectiva “de facto” de Anu Bradford

De acordo com Anu Bradford (2020, p. 142-145), a indivisibilidade dos dados pessoais é uma característica que contribui para que haja uma tendência à adoção de legislação similar à RGPD em outros ordenamentos - essa indivisibilidade nada mais é do que a dificuldade desses atores optarem por abandonar o mercado europeu para não se sujeitarem às condições impostas pela regulação ou, ainda, a dificuldade de diferenciar dados pessoais de indivíduos localizados em território europeu dos demais, gerando um tratamento diferenciado aplicável a cada jurisdição. São os custos de uma customização que tornam a divisibilidade impraticável, de modo que as empresas acabam optando por seguir a norma mais restritiva - como é o caso do RGPD - em todos os lugares, conforme expõe Bradford[7]:

> Se o Efeito Bruxelas ocorre, portanto, muitas vezes se resume à questão da não divisibilidade dos produtos e serviços entre os usuários globais. Vários exemplos sugerem que, para as empresas digitais globais de hoje, manter diferentes práticas de dados nos mercados globais é muitas vezes difícil (devido à não divisibilidade técnica) e caro (devido à não divisibilidade econômica). É imperativo que essas empresas sejam capazes de mover dados sem problemas através das fronteiras, em particular, pois geralmente armazenam seus dados em servidores localizados em mercados diferentes daqueles em que operam. Embora as regulamentações de privacidade possam diferir de jurisdição para jurisdição, essas as empresas digitais simplificam seus sistemas globais de gerenciamento de dados para reduzir seus custos de conformidade com vários regimes regulatórios. Em vez de criar programas diferentes para diferentes mercados, elas tendem a aplicar os padrões mais rigorosos em geral. Às vezes, é tecnologicamente difícil, até mesmo impossível, separar dados envolvendo cidadãos europeus e não

[7] No original, “Whether the Brussels Effect occurs therefore often comes down to the question of non-divisibility of the products and services across global users. Various examples suggest that, for today’s global digital companies, maintaining different data practices across global markets is often both difficult (due to technical non-divisibility) and costly (due to economic non-divisibility). It is imperative that these companies are able to move data seamlessly across borders, in particular, as they often store their data in servers that are located in markets different from those where they operate.82 While privacy regulations may differ from jurisdiction to jurisdiction, these digital companies streamline their global data management systems to reduce their compliance costs with multiple regulatory regimes.83 Instead of creating different programs for different markets, they tend to apply the most stringent standards across the board.84 At times, it is technologically difficult, even impossible, to separate data involving European and non-European citizens.85 Other times it may be feasible, but too costly, to create special websites or data processing practices just for the EU.86 As a result, the technical or the economic non-divisibility of the EU rules has prompted several US companies ranging from Google to Netflix to amend their global privacy practices. 7 When opting for a single global policy, these companies typically choose to adopt the most stringent regulation so as to retain the ability to conduct business everywhere.”

> europeus. Outras vezes pode ser viável, mas muito caro, criar sites especiais ou práticas de processamento de dados apenas para a UE. A divisibilidade das regras da UE levou várias empresas dos EUA, do Google à Netflix, a alterar suas práticas globais de privacidade. Ao optar por uma única política global, essas empresas geralmente optam por adotar a regulamentação mais rigorosa para manter a capacidade de conduzir negócios em todos os lugares. (BRADFORD, 2020, p. 142-143, tradução livre)

Outros fatores que podem também indicar esse comportamento são a necessidade de empresas globais conduzirem seus negócios internamente de acordo com um padrão para facilitar processos internos e prestações de contas, além de para fins reputacionais e de marca, a fim de não justificar porque determinados consumidores teriam direito a um tratamento de seus dados pessoais mais restritos e outros menos (BRADFORD, 2020, p. 144-145).

A respeito dessa demanda que é imputada às empresas, Flávia Piovesan e Victoriana Gonzaga afirmam que a promoção de direitos pelo setor privado – e, neste caso, de defesa de normas de proteção de dados pessoais - não trazem apenas ganhos em termos monetários, mas também de ganhos reputacionais e de competitividade, conforme disposto a seguir:

> Da mesma forma, promover direitos simboliza não apenas um alto ganho empresarial (como já mencionado, estudos apontam o quanto a diversidade é lucrativa), mas sobretudo um ganho na identidade e reputação empresarial, por meio da melhoria da imagem pública e agregação de valor à marca. A empresa ganha, ainda, em temos de competitividade (gerando resultados econômicos positivos para o país), com atração de investidores; fidelização de clientes e beneficiários; atração e permanência dos funcionários; bem como com a redução de litígios por violação de direitos e conflitos envolvendo partes interessadas e comunidade local. (PIOVESAN, GONZAGA, 2019, p. 26).

Inclusive, diversas empresas que conduzem seus negócios no Brasil mantêm em seus termos de uso e suas políticas de privacidade diretrizes compatíveis com a LGPD e com o RGPD, além dos casos em que há a menção expressa da aplicabilidade da norma, como a Apple e o Facebook, por exemplo[8]:

> Os aplicativos também devem fornecer ao cliente uma maneira facilmente acessível e compreensível de retirar o consentimento. Certifique-se de que suas strings de propósito descrevam de forma clara e completa o uso dos dados. Os aplicativos que coletam dados para um interesse legítimo sem consentimento,

[8] No original, “Apps must also provide the customer with an easily accessible and understandable way to withdraw consent. Ensure your purpose strings clearly and completely describe your use of the data. Apps that collect data for a legitimate interest without consent by relying on the terms of the European Union’s General Data Protection Regulation (“RGPD”) or similar statute must comply with all terms of that law.”

> baseando-se nos termos do Regulamento Geral de Proteção de Dados da União Europeia (“RGPD”) ou estatuto semelhante, devem cumprir todos os termos dessa lei. (APPLE, 2022, item 5.1.1.ii, tradução livre)

> Compartilhamos informações globalmente, tanto com as Empresas da Meta quanto com os nossos parceiros e com quem você se conecta e compartilha no mundo todo, em conformidade com esta política. Suas informações podem, por exemplo, ser armazenadas e tratadas nos Estados Unidos ou em outros países fora de onde você mora ou transferidas ou transmitidas a esses lugares para os fins descritos nesta política. Essas transferências de dados são necessárias para oferecer os serviços estipulados nos Termos da Meta e nos Termos do Instagram, bem como para operar em todo o mundo e fornecer nossos Produtos a você. Usamos cláusulas-padrão contratuais, seguimos as decisões de adequação da Comissão Europeia sobre determinados países, quando aplicável, e obtemos seu consentimento para essas transferências de dados aos Estados Unidos e outros países. (META, 2022)

3.2 O teor normativo da LGPD e a análise da influência do RGPD sob a perspectiva “de jure” de Anu Bradford

O PL 4060/2012 resultou, após anos de discussão e alterações, em uma complexa LGPD composta por sessenta e cinco artigos que estabelecem desde as definições de dado pessoais e dados pessoais sensíveis, perpassam as formas de tratamentos desses dados, os direitos de seus titulares, as sanções aplicáveis em caso de descumprimento da lei, até a criação de um órgão específico da administração pública federal responsável pela fiscalização da lei e outras competências descritas na norma (a ANPD).

Ainda que tenha contado com adaptações e adequações culturais, econômicas, linguísticas e qualitativas óbvias, a LGPD tem extensas semelhanças com o RGPD (ONETRUST DATAGUIDANCE, BAPTISTA LUZ ADVOGADOS, 2019; LGPD ACADÊMICO, 2020), refletindo a intenção de harmonização nacional quanto ao referido ordenamento internacional, conforme mencionado na descrição da relatoria do Deputado Orlando Silva (PCdoB-SP) para aprovação do PL 4060/2012 abordada acima.

Evidentemente, há diferenças relevantes entre as normativas, especialmente por se tratar de espécies jurídicas diferentes. A LGPD é uma lei ordinária, promulgada internamente e, portanto, restrita ao território brasileiro. Já o RGPD é um regulamento, possuindo caráter geral e sendo obrigatório aos Estados-Membros e instituição da EU, prescindindo de um ato nacional de transposição por esses Estados (PARLAMENTO EUROPEU, 2022, p. 3).

Contudo, há também diversas semelhanças. Ambas as legislações se aplicam a organizações locais e também àquelas organizações estrangeiras que tratam dados pessoais nessas e oriundos das regiões de suas jurisdições, dividem o papel e a responsabilidade pelo tratamento de dados pessoais entre processadores e controladores, criam a obrigação de organizações apontarem um “encarregado” pelo tratamento de dados pessoais (também conhecido como DPO, conforme atribuído pelo RGPD) e conduzir avaliações de impacto à proteção de dados pessoais, na medida de suas atividades. Ambas também trazem a figura de uma autoridade governamental (no caso da LGPD, a ANPD e, no caso do RGPD, as Autoridades de Proteção de Dados) para fiscalização e aplicação da lei.

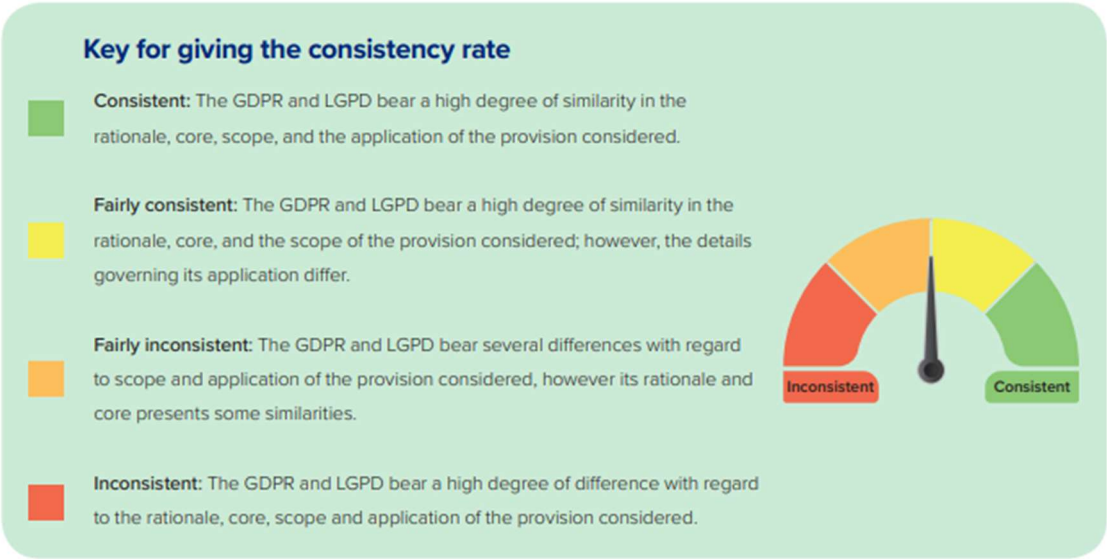
Por outro lado, há diferenças entre as legislações. O RGPD, por exemplo, permite que estados-membros da UE modulem uma de suas regras e obtenham consentimento de menores de, no mínimo, 13 anos de idade diretamente (em regra, a idade mínima prevista é de 16 anos). Qualquer consentimento de indivíduo que não tenha alcançado essas idades deve ser concedido pelo responsável legal da criança ou adolescente. A LGPD, por sua vez, prevê que o consentimento quanto ao tratamento de seus dados pode ser dado por indivíduo entre 13 e 18 anos, desde que realizado no interesse do menor. Em idades inferiores, o consentimento deve ser dado pelo responsável legal (ONETRUST DATAGUIDANCE, BAPTISTA LUZ ADVOGADOS, 2019, p. 18).

Tanto a LGPD quanto o RGPD preveem a aplicação de sanções pecuniárias em caso de descumprimento, embora cada uma tenha valores, sujeitos e natureza das penalidades próprias (ONETRUST DATAGUIDANCE, BAPTISTA LUZ ADVOGADOS, 2019, p. 48-49). Outro exemplo é o de que o tratamento de dados pessoais por órgãos de pesquisa é mais flexível sob o RGPD em comparação à LGPD - enquanto a primeira prevê que o processamento de dados para pesquisa científica deve possuir uma interpretação abrangente, a segunda restringe o tratamento dos dados internamente ao órgão (ONETRUST DATAGUIDANCE, BAPTISTA LUZ ADVOGADOS, 2019, p. 20-21).

Um estudo conduzido por um escritório de advocacia Baptista Luz Advogados, avaliou que, dentre 24 matérias tratadas na lei e distribuídas nos temas escopo, definições, base legal de tratamento de dados pessoais, obrigações de controladores e processadores, direitos dos titulares e *enforcement* da lei, 15 matérias são “razoavelmente similares”, 8 matérias são “razoavelmente inconsistentes” entre si e 1

é “inconsistente”, de acordo com os critérios de avaliação abaixo (ONETRUST DATAGUIDANCE, BAPTISTA LUZ ADVOGADOS, 2019):

Figura 1 – Critérios de avaliação de semelhança entre as disposições do RGPD e LGPD



Fonte: ONETRUST DATAGUIDANCE, BAPTISTA LUZ ADVOGADOS, 2019, p. 6.

Outro estudo conduzido pelo LGPD Acadêmico (2020, conforme Anexo C), um repositório digital fomentado por profissionais operadores do direito, tecnologia, compliance, estudantes e voluntários para compartilhamento de conhecimento acerca da privacidade, avalia quais atividades de gerenciamento de privacidade e proteção de dados pessoais (por exemplo, a obrigação de atribuir a responsabilidade pela privacidade e proteção dos dados a um indivíduo, como o DPO) estão presentes na LGPD e no RGPD.

No estudo, essas atividades são distribuídas em 13 grandes categorias que representam as obrigações previstas em lei, como manter estrutura de governança, manter a política de privacidade e proteção de dados, manter programa de treinamento e conscientização, gerenciamento de riscos de terceiros, monitoramento de tratamento de dados, dentre outras. Dentre 83 atividades de gerenciamento previstas no RGPD, 65 delas estão refletidas na LGPD (LGPD ACADÊMICO, 2020 – conforme Anexo C).

Além das comparações acima, é relevante analisar se os princípios basilares do RGPD, que servem de fundamento para as demais previsões da lei (inclusive, por exemplo, as previsões que definem as atividades de gerenciamento de privacidade e

tratamento de dados pessoais exigidas legalmente e apontadas no Anexo C), encontram correspondência na LGPD, a fim de aferir se as bases que as suportam são correspondentes, apesar das diferenças de natureza jurídica, redacionais e até mesmo culturais das referidas normas.

Para tanto, a tabela a seguir é apresentada com o objetivo de sistematizar os princípios norteadores encontrados em cada uma das leis e atribuir um grau de semelhança a cada um deles, com base na seguinte gradação: ao princípio que for atribuída a cor verde na coluna “grau de semelhança”, entende-se que há uma grande correspondência entre as leis; ao que for atribuída a cor amarela, entende-se que há uma média correspondência entre as leis; e, ao que for atribuída a cor vermelha, entende-se que não há correspondência entre as leis.

Aqui cabe uma ressalva: a sistematização abaixo não pretende interpretar juridicamente cada princípio, buscando previsões compatíveis com eles em cada uma das leis, mas tão somente identificar se as regras indicadas como princípios basilares por uma norma são também indicadas como princípios fundamentais também na outra norma. Dessa forma, é possível, por exemplo, que determinado princípio de uma norma seja encontrado no texto de outra, mas não esteja explicitamente indicado como um princípio nesta última, razão pela qual atribuir-se-á um baixo grau de correspondência ao referido princípio.

Quadro 2 - Comparação de princípios basilares previstos no RGPD e LGPD

Princípio	Disposição do RGPD	Disposição da LGPD	Grau de semelhança
Licitude	O tratamento de dados pessoais deve ser lícito (Art. 5º, 1.a)	As atividades de tratamento de dados pessoais devem ser conduzidas de boa-fé e de acordo com o princípio da não discriminação (isto é, sem fins discriminatórios ilícitos ou abusivos) (Art. 6º, *caput* e inciso IX)	
Razoabilidade	O tratamento de dados pessoais deve ser razoável (Art. 5º, 1.a)	A compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento. (Art. 6º, inciso II)	
Transparência	O tratamento de dados pessoais deve ser transparente (Art. 5º, 1.a)	Deve-se garantir aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento de dados pessoais (Art. 6º, inciso VI)	

Livre acesso		A 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; (Art. 6º, inciso IV)	
Finalidade	O tratamento de dados pessoais deve ser realizado para finalidade determinada, explícita e legítima (Art. 5º, 1.b)	O tratamento de dados pessoais deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular (Art. 6º, inciso I).	
Minimização dos dados	O tratamento de dados pessoais deve ser adequado, pertinente e limitados ao que é necessário para se atingir à finalidade para a qual é tratado (Art. 5º, 1.c)	Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; (Art. 6º, inciso III).	
Exatidão	Os dados pessoais tratados devem ser exatos, atualizados sempre que necessário, apagados ou retificados em caso de inexatidão (Art. 5º, 1.d)	Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; (Art 6º, inciso V)	
Limite de conservação	Os dados pessoais tratados devem ser conservados apenas pelo período necessário para que as finalidades para as quais são tratados sejam atingidas, ou por períodos mais longos para fins de arquivo de interesse público, investigação científica ou histórica ou para fins estatísticos. (Art. 5º, 1.e)	Sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (Art. 6º, inciso I)	
Integridade	Os dados pessoais devem ser tratados de forma que garanta a sua segurança e os proteja de perdas, destruição ou dano. (Art. 5º, 1.f)	Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoaisde situações acidentais ou ilícitas de destruição, perda ou alteração (Art. 6º, inciso VII)	
Confidencialidade	Os dados pessoais devem ser tratados de forma que	Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de	

	garanta a sua segurança e impeça o seu tratamento não autorizado ou ilícito. (Art. 5º, 1.f)	acessos não autorizados, situações acidentais ou ilícitas de comunicação ou difusão. (Art. 6º, inciso VII)	
Prevenção		adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; (Art. 6º, inciso VIII)	
Responsabilidade	Quem realiza o tratamento de dados pessoais é responsável por cumprir e comprovar o cumprimento dos princípios anteriormente elencados. (Art. 5º, 2)	Quem realiza o tratamento de dados pessoais é responsável por adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (Art. 6º, inciso X)	

Legenda da coluna “grau de semelhança”: verde – grande correspondência entre as leis; amarelo – média correspondência entre as leis; vermelho - não há correspondência entre as leis.
Fonte: Elaborado pela autora.

A partir da tabela acima, é possível notar que, guardadas as proporções, redações e especificidades de cada norma, a maior parte dos princípios de ambas as leis possuem alto grau de semelhança.

Também quanto à semelhança dos princípios de cada lei, Beatriz Graziano Chow e Clarisse Laupman Ferraz Lima (2021, p. 312) apontam que:

> Há dois aspectos-chave da lei que vale a pena mencionar nestas breves observações de ambas as legislações. A primeira é a hipótese de aplicação extraterritorial do RGPD e da LGPD e a segunda são os princípios que orientam ambas. Seus princípios também são muito semelhantes. O RGPD exige legalidade; justiça; transparência; limitação de dados; precisão; limitação de retenção; integridade e confidencialidade (segurança da informação) e responsabilidade, para citar alguns. Quanto à LGPD, há também muitos [princípios] relevantes, [a lei] garante a boa-fé; a finalidade do processamento; compatibilidade do tratamento com as finalidades informadas ao titular dos dados; limitação do processamento ao mínimo necessário para cumprir suas finalidades; transparência aos titulares dos dados; uso de medidas técnicas e administrativas para proteger dados pessoais; e responsabilidade. [9] (CHOW, LIMA, 2021, p. 312, tradução livre)

[9] No original, “There are two key aspects of the law worth mentioning in these brief remarks of both legislations. The first one is the hypothesis of extraterritorial application of the RGPD and the LGPD and the second one is the principles that guide them both. Their principles are also very similar. The RGPD demands lawfulness; fairness; transparency; data limitation; accuracy; limitation of retention; integrity and confidentiality (information security) and accountability, to name a few. As for the LGPD, there are also many relevant ones, it ensures good faith; the purpose of the processing; compatibility of the processing with the purposes informed to the data subject; limitation of the processing to the

Assim, a diferença entre as normas parece muito mais estar nas nuances de seus dispositivos do que em uma diferença de perspectiva da legislação quanto à forma de tratamento e proteção de dados pessoais.

De acordo com Daniel Michaels, a maioria dos 120 países que possuem leis de privacidade adotou normativas parecidas com o RGPD europeia tal como Japão, África do Sul, Colômbia, Tailândia, Coreia do Sul e, como visto acima, o Brasil (MICHAELS, 2018; SCOTT; CERULUS, 2018; PORNWASIN, 2018).

Essa imitação da lei europeia se dá por diversos motivos. Um deles é o fato de que muitos países optam por seguir a norma com padrão mais alto e amplamente aceito. Outro fator é o de que, como grandes empresas já estavam sujeitas à RGPD, governos encontram menos dificuldades em aplicar a mesma lei localmente (BRADFORD, 2020, p. 148 - 149).

Há também o entendimento de que a adoção de uma normativa semelhante à norma estrangeira já existente foi entendida como vantajosa pelo setor privado, a fim de reduzir eventuais custos com uma nova regulação internacional, conforme mencionado no capítulo anterior (ALVES, item 4).

Bradford (2020, p. 148 - 149) ainda aponta que esses países desejam que seu ordenamento de proteção de dados pessoais seja considerado “adequado” aos olhos da UE e, portanto, não sofra as consequências de possuir um regime que não confira um nível de proteção compatível e possivelmente impacta o fluxo internacional de dados pessoais, conforme previsto no Capítulo 5 do RGPD e abordado no tópico 3.1 acima. Caso não possuam essa adequação, as empresas que tratam dados pessoais precisam recorrer a alternativas, conforme exposto a seguir:

> Se um país em que uma empresa opera não tiver um nível adequado de proteção de dados, as empresas que ainda desejam transferir dados para esse país devem obter a aprovação de uma autoridade supervisora competente para as Regras Corporativas Vinculantes (BCR). Essas regras estabelecem as obrigações de proteção de dados para todas as entidades desse grupo corporativo. Se essas BCRs forem aprovadas, elas funcionarão como uma lei de proteção de dados aprovada pela UE para essa empresa específica. Alternativamente, essas empresas podem usar “cláusulas contratuais padrão” aprovadas pela UE. Essas cláusulas permitem que as empresas celebrem um contrato com entidades da UE e se comprometam a cumprir as regras de privacidade da UE, oferecendo uma “solução” para

---

minimum necessary to fulfill its purposes; transparency to data subjects; use of technical and administrative measures to protect personal data; and accountability.”

> empresas nos casos em que o país não possui leis de proteção de dados adequadas.[10] (BRADFORD, 2020, p. 149-150, tradução livre)

De acordo com Beatriz Graziano Chow e Clarisse Laupman Ferraz Lima, o "efeito dominó" das regulamentações de dados pessoais pode ser explicado pela extraterritorialidade – ou seja, pelo alcance da lei fora de seus territórios nacionais ou jurisdições, ultrapassando as fronteiras europeias e alcançando países como o Brasil (CHOW; LIMA, 2021, p. 304).

Assim, a adoção da LGPD em semelhança à RGPD conclui o impacto da teoria do "Efeito Bruxelas" de Anu Bradford sob a perspectiva *de jure* (2020, p. 147-155). Essa incorporação de uma norma à semelhança de uma regulação estrangeira levanta também questionamentos sobre a possibilidade desse movimento possuir implicações nas áreas das Relações Internacionais e do Direito, conforme será discutido nos capítulos subsequentes.

4 A DIFUSÃO INTERNACIONAL DE NORMAS E A RUPTURA DAS VISÕES TRADICIONAIS DO SISTEMA INTERNACIONAL

Conforme tratado nos capítulos anteriores, a promulgação da LGPD trilhou um caminho que perpassa a preocupação da sociedade global com a proteção de dados pessoais, a adoção de regulamentação específica pela UE e outros Estados – tendo esta assumido um papel de *agenda-setter* a respeito do tema – e a mobilização de diferentes setores e entes da sociedade acerca da pauta (inclusive o setor empresarial), até culminar na acomodação de interesses e adoção oficial de uma regulamentação de proteção de dados pessoais pelo Brasil.

Embora a visão geral desse percurso, quando realizada à distância e neste momento que já é posterior à promulgação da lei, possa trazer uma impressão de objetividade, a realidade é que o movimento foi permeado de negociações, debates e

[10] No original, "If a country in which a company operates has not been deemed to have an adequate level of data protection, companies that still want to transfer data to that country must seek approval from a competent supervisory authority for Binding Corporate Rules (BCR). These rules set out the data protection obligations for all the entities in that corporate group.142 If these BCRs are approved, they function as an EU-approved data protection law for that particular company.143 Alternatively, these companies can use "standard contractual clauses" approved by the EU.144 These clauses allow companies to enter into a contract with EU entities and pledge to meet the EU's privacy rules, offering a "workaround" for companies in instances where the country does not have adequate data protection laws."

rupturas entre os entes que atuaram no processo legislativo, cujos interesses eram os mais diversos em diferentes pontos e proposições da lei.

De um lado houve a participação de entes cujos interesses eram voltados à proteção dos consumidores e defendiam a atribuição de mais responsabilidades aos processadores de dados pessoais, como, por exemplo, o IDEC. De outro lado, certas associações representativas de empresas privadas ou grandes corporações buscavam a adoção de uma lei cujo teor possuísse uma flexibilidade capaz de não limitar o desempenho da atividade empresarial. Mas esse posicionamento divergente não necessariamente ocorria acerca de todo e qualquer ponto da proposta de lei ou foi definitivo – em determinados momentos ou a depender do assunto, participantes de lados a princípio opositores podem passar a defender uma mesma opinião, oposta até mesma ao entendimento de participantes que, até então, eram aliados.

Inclusive, a existência de uma coalizão multissetorial em defesa da aprovação da lei, evidenciada por meio da assinatura do Manifesto pela Aprovação da Lei de Proteção de Dados Pessoais (BRASSCOM, 2018), que contou com o apoio de entidades representativas, comunidade acadêmica, indivíduos e organizações privadas, conforme descrito no Anexo B, explicita que o caminho até a promulgação da LGPD foi também marcado por consensos.

Além dessa dinâmica participativa visível, a análise do processo legislativo da LGPD sob a ótica de Anu Bradford dá sinais de algumas motivações reiteradamente expostas como base para adoção da lei: a necessidade de o Brasil possuir uma legislação compatível com a da UE, as vantagens de adotar uma norma considerada adequada ou aceitável aos olhos de outros países e atores econômicos, a atenção em aproveitar os benefícios econômicos que o mercado de tecnologia auferiria em virtude da adoção da lei, reduzir os malefícios ou riscos sociais e econômicos em caso de não adoção de uma norma e, ainda, até mesmo a tentativa de a EU sujeitar entidades de outros territórios à observância de sua legislação[11].Essas justificativas demonstram a influência de atores e narrativas que, ainda que não necessariamente representadas formalmente por meio de um participante específico, atuaram como uma espécie de força invisível traduzida nas motivações dos diferentes atores participantes do processo legislativo da LGPD.

[11] Isso porque, conforme visto nos capítulos anterior, o RGPD prevê que, é vedado o tratamento de dados pessoais por empresa não esteja em um país capaz de assegurar um nível de proteção equivalente ao da UE (seja por força de lei ou por meio da assunção de compromissos contratuais específicos de proteção) (UE, art. 44-50).

Essa dança de interesses e influências transportadas por uma pluralidade de atores – que não são apenas governos, mas também, como visto acima, empresas, comunidade científica e associações representativas de interesses diversos – implicam em tomadas de decisões que repercutem transnacionalmente. Essa é a dinâmica da Governança Global, fenômeno conceituado como os processos de governança existentes em um mundo globalizado que deixou de ser visto como governado tão somente por governos ou estados nacionais e impactos locais, mas sim por uma diversidade de atores e fatores cujas decisões tomadas em um local podem impactar outros, ainda que distantes (FINKELSTEIN, p. 367-372; ROSENAU, p. 144-145).

Assim, conforme descrito a seguir, James Rosenau (1997, p. 144) expõe que a Governança Global é um termo que busca resumir as complexas ações que culminam no formato em que o mundo funciona atualmente, tendo como característica fundamental a pluralidade de atores e o deslocamento de autoridades tradicionalmente vistas como governantes.

> A governança global não é tanto um rótulo para um alto grau de integração e ordem, mas um termo resumido para atividades altamente complexas e amplamente díspares que culminam em um mínimo de coerência mundial. A soma das atividades díspares e muitas vezes conflitantes pode ser considerada como uma ordem mundial emergente, mas é uma ordem apenas no sentido de que descreve a maneira como as coisas funcionam atualmente na arena política. Avaliado na perspectiva de um conjunto integrado e harmonizado de arranjos, o mundo emergente é marcado por um alto grau de desordem e turbulência.
> (...)
> Como ponto de partida, a governança é aqui concebida em um nível muito abstrato como esferas de autoridade (SOAs) em todos os níveis de atividade humana - do lar ao público exigente e à organização internacional - que equivalem a sistemas de governo nos quais os objetivos são perseguidos através do exercício do controle. A razão para esta ampla formulação é simples: em um mundo turbulento e cada vez mais interdependente, onde o que acontece em um canto ou em um nível pode ter consequências para o que ocorre em todos os outros cantos e níveis, parece um erro aderir a uma estreita definição em que apenas as instituições formais nos níveis nacional e internacional são consideradas relevantes. [12] (ROSENAU, 1997, p. 144, tradução livre)

[12] No original, “Global governance is not so much a label for a high degree of integration and order as it is a summary term for highly complex and widely disparate activities that culminate in a modicum of worldwide coherence. The sum of the disparate and often conflicting activities can be regarded as an emergent world order, but it is an orderliness only in the sense that it depicts the way things currently work in the political arena. Assessed from the perspective of an integrated and harmonized set of arrangements, the emergent world is marked by a high degree of disorder and turbulence. As a point of departure, governance is here conceived at a very abstract level as spheres of authority (SOAs) at all levels of human activity - from the household to the demanding public to the international organization - that amount to systems of rule in which goals are pursued through the exercise of

Esse cenário permite que regras sejam institucionalizadas em um formato “top-down”, onde cada Estado Nacional ou figura governante institucionalmente reconhecida é responsável por criar e impor suas estruturas, bem como em um formato “bottom-up” cuja institucionalização é indireta e impulsionada por atores que experenciam interações ou atividades que acabam culminando em controles institucionalizados (ROSENAU, 1997, p. 156).

Enquanto podemos ver sinais do primeiro formato na tradicional ordem internacional, por meio da qual Estados negociam bilateralmente (STONE, 2004, p. 546) entre si, aderem a tratados e eventualmente os internalizam, o segundo modelo é visto na difusão internacional de políticas – como é o caso da difusão de uma regulamentação de proteção de dados pessoais pela UE (por meio da promulgação do RGPD) ao Brasil (por meio da promulgação da LGPD).

Essa transferência de políticas permite que normas, instituições e ideias implementadas em determinado local sejam utilizadas no desenvolvimento de normas, instituições e ideias de outro local, implicando em uma transferência de conhecimento entre diferentes momentos da história e dentro ou entre diferentes países (STONE, 2004, p. 545; DOLOWITZ; MARSH, 2000, p. 5), podendo ocorrer por meio da reprodução, sintetização, adoção híbrida de políticas, normas e técnicas, ou ainda inspiração nestes diplomas (DOLOWITZ; MARSH, 1996, p. 351).

De acordo com Diane Stone (2004, p. 545-550), atores não estatais como grupos de interesses, organizações não governamentais, consultorias, bancos e *thinktanks* tem um papel chave nessa difusão de políticas, atuando como representantes de interesses que impulsionam a transferência de normas.

Esse complexo emaranhado de atores e dinâmicas que circundam à tomada de decisões na sociedade atual não interessa apenas ao universo das Relações Internacionais, mas possui também reflexos e impactos no Direito.

Primeiro porque o Direito, assim como as Relações Internacionais, estuda esse movimento de transferência de normas através de diferentes perspectivas, dentre elas as teorias de direito comparado que, por meio do uso de metáforas como “transplantes”, “transferência”, “empréstimos” e “migrações” de normas e ideias com

---

control. The reason for this broad formulation is simple: in a turbulent and ever more interdependent world, where what happens in one corner or at one level may have consequences for what occurs at every other corner and level, it seems a mistake to adhere to a narrow definition in which only formal institutions at the national and international levels are considered relevant.”

impactos jurídicos, buscam estudar mecanismos por meio dos quais normas se difundem internacionalmente (PERJU, 2012, p. 3).

Segundo porque o movimento de difusão internacional de normas desafia visões tradicionais a respeito da organização da ordem jurídica internacional e a relação entre direito interno e direito internacional, uma vez que a da primordialidade de Estados soberanos conforme trazido na ordem de Vestfália passou a concorrer com uma pluralidade de outros atores que possuem alguma autoridade (WALKER, 2002, p. 334). Ambas as motivações aqui apontadas passam a ser explorados mais detalhadamente a seguir.

Com relação ao primeiro motivo, Watson conceitua como “transplante jurídico” o mecanismo que permitiria a mudança de regras (ou melhor, ideias), de um país ou povo para outro (WATSON, 1993, p. 21-30). Segundo o autor, o mecanismo é tão visível no mundo moderno - podendo ser notado a partir do fato de que a maioria dos ordenamentos jurídicos do mundo ocidental derivam do Direito Romano - quanto no mundo antigo - vez que o Código de Humarabi, Exodus e Eshnunna teriam disposições bastante similares -, por meio de recepções voluntárias, imposições e os mais diversos formatos e dimensões que levem à efetivação do transplante (WATSON, 1993, p. 22-24).

Watson ainda destaca que o mecanismo dos transplantes é facilmente empregado porque, na sua visão, normas jurídicas são autônomas de um contexto social e cultural (PERJU, 2012, p. 3), o que permitiria que elas viajassem por meio de três principais eventos: a partir do deslocamento populacional de indivíduos sujeitos a uma determinada norma para outro território cuja civilização não é comparável, a partir do deslocamento populacional de indivíduos sujeitos a uma determinada norma para outro território cuja civilização é comparável e, por fim, quando a população voluntariamente aceita o sistema de outros povos (WATSON, 1993, p. 29-30).

Teorias subsequentes a dos “transplantes jurídico” trazem uma relação mais próxima entre normas jurídicas e contexto econômico, social e cultural que aquela apresentada anteriormente, indicando que a dinâmica de trocas e circulação de normas não é um evento isolado, mas que uma migração normativa é permitida por estar associada a uma multiplicidade de discursos e fatores que levam a uma convergência e, ao fim, à adoção (não necessariamente idêntica ou em sua integralidade) da norma. Esses fatores compreendem convergência quanto ao objeto

em discussão, fatores temporais, motivações e padrões de proximidade, tais como cultura, história e ideologia) (PERJU, 2012, p. 4-5).

No estudo deste trabalho, por exemplo, nota-se uma grande compatibilidade entre o RGPD e a LGPD no que tange ao objeto das normas, o tempo da promulgação de cada uma delas, as motivações que levaram à adoção de ambas e outros padrões convergentes nos contextos em que cada uma delas se insere – como visto nos capítulos anterior cujo foco é a análise do processo legislativo da LGPD, a norma possui diversas semelhanças e convergências com o RGPD, refletindo o fenômeno da migração de uma norma na prática.

Não se pode, ainda, ignorar que, embora haja pontos de convergência entre o RGPD e a LGPD, bem como entre outras normas que podem ser analisadas sob a ótica comparativa, elas não são idênticas justamente por haver uma aculturação – seja em suas palavras ou em sua interpretação. Assim, de acordo com Pierre Legrande (2014, p. 22-24), não há uma transplantação literal de normas, mas sim um cenário de surgimento de diferentes normas, no seguinte cenário:

> O comparatista deve adotar uma visão do Direito como um significante polissêmico que conota referentes culturais, políticos, sociológicos, históricos, antropológicos, linguísticos, psicológicos e econômicos, inter alia. A tomar emprestado de Mauss, cada manifestação do Direito – cada regra, por exemplo – deve ser percebida como um fait social total, um fato social total.
> Dessa forma, nada indica que as mesmas palavras inscritas gerarão a mesma ideia em uma cultura diferente, a fortiori se as palavras inscritas são elas próprias diferentes porque foram declaradas em outra língua. (Como Benjamin escreveu: “[...] a palavra Brot significa algo diferente para um alemão do que a palavra pain para um francês”.)
> Assim, o transplante não acontece de fato: uma característica fundamental da regra – seu significado – fica para trás, de modo que a regra que estava lá, com efeito, não é deslocada para cá. Pressupondo uma linguagem comum, a posição é a seguinte: havia uma regra (palavras inscritas a + significado x), e agora há uma segunda regra em outro lugar (palavras inscritas a + significado y). Não é a mesma regra. (A diferenciação entre concepções de Direito não é superada.). (LEGRANDE, 2014, p. 22-24).

Assim, independentemente da terminologia adotada para explicar o mecanismo de “migração” de normas, o objetivo desta discussão é destacar que, embora transferências de normas não necessariamente produzam efeitos idênticos em diferentes culturas (por exemplo, a LGPD, embora claramente semelhante à RGPD, possui diversas disposições com uma abordagem mais ou menos conservadora ou simplesmente diferente, conforme tratado acima), essas “transferências jurídicas são possíveis, estão ocorrendo, já ocorreram e continuarão ocorrendo.” (NELKEN, 2003,

p. 437). E continuarão ocorrendo de forma ainda mais intensa, já que o fenômeno da globalização traz maior interação e interdependência entre territórios.

Nesse sentido, deve-se preocupar com os contextos, o nascimento e a consolidação das regras jurídicas, bem como análisa-los sempre lembrando que são fenômenos jurídicos e sociais, e não atos isolados. Antonio Sánchez-Bayón defende que essa aproximação entre teoria e prática é primordial para que se possa analisar as transformações de fatores e paradigmas jurídicos geradas pela globalização e que impulsionam o surgimento de um direito que deixa de ser doméstico ou internacional, mas torna-se o que o autor chama de “direito transnacional” ou “direito global” (2012, p. 147,), superando-se um positivismo formalista estatal e abrindo a possibilidade para uma análise subjetiva das normas que considera critérios temporais, espaciais, materiais, culturais, dentre outros, podendo-se também observar intencionalmente as interações normativas entre os diferentes ordenamentos (2012, p. 17).

Esse desfecho nos leva ao segundo motivo de impacto da difusão de normas no Direito: o desafio às teorias tradicionais a respeito da ordem jurídica internacional e a relação entre direito interno e direito internacional.

Tradicionalmente, o sistema institucional e normativo internacional possui seus fundamentos na Paz de Vestfália – apelido que se dá ao contexto de celebração dos Tratados de Münster e Osnabruque de 1648, marco histórico que delimita o fim da Guerra dos Trinta Anos -, o qual destaca o Estado, dotado de soberania e independência perante seus pares, como o meio e a ferramenta por meio da qual o direito internacional opera (ACIOLLY; CASELLA; SILVA, p. 100-101).

Tendo o Estado como protagonista das relações internacionais, estudiosos do Direito refletem acerca da relação entre direito interno e direito internacional com debates que normalmente giram em torno de duas teorias, a monista e a dualista.

A teoria dualista, em sua origem, argumenta que direito interno e direito internacional são sistemas diferentes e independentes, vez que se destina a regular a relação entre Estados e, portanto, se estendia somente a estes (ALVARADO, 2016, p. 18). Assim a visão mais radical dessa teoria entende que, para que o direito internacional tenha efeito sob os indivíduos, ele deve ser aceito internamente e incorporado como uma lei interna (TRIEPEL, 1923, p. 73-122), conforme procedimentos legislativos previstos pelas leis do referido local. A visão mais branda, por sua vez, entende que uma incorporação formal de eventual norma internacional por meio de lei não é imprescindível (ACIOLLY, CASELLA e SILVA, 2012, p. 228).

Já a teoria monista entende que o ordenamento jurídico é algo único e indivisível, não havendo separação entre direito interno e internacional, de forma que o direito internacional não necessita de nenhum ato especial para ser observado internamente pelos indivíduos daquele território (KELSEN, 1927). Esse debate levanta então uma questão de hierarquia, havendo duas visões: a de que o direito internacional prevaleceria sobre o direito nacional, já que o reconhecimento do próprio ordenamento interno depende do direito internacional para sua existência, ou a de que o direito nacional prevaleceria sobre o internacional, tendo em vista sua soberania (ALVARADO, 2016, p. 19).

Essas vertentes, porém, acabam sendo limitadas quando observadas dentro de um contexto de difusão internacional de normas, já que limitam o direito internacional à negociação e acordos entre Estados e dão demasiada importância à soberania desses Estados para que normas internacionais sejam reconhecidas nacionalmente, trazendo tratados internacionais, organizações internacionais e a diplomacia como impulsionadores da difusão de normas da ordem internacional para a ordem doméstica (BRADFORD, 2020, p. 74), trazendo a impressão de existir uma “hierarquia”.

Estes fatores desconsideram a diversidade de atores envolvidos nas dinâmicas de criação, negociação, promulgação e difusão de normas, além das diferentes instituições nas quais esses atores convivem e que não se resumem à nível nacional ou nível internacional, cenário que deriva da globalização e do capitalismo, tendo em vista que esses fenômenos trazem o rompimento de barreiras fronteiriças na circulação de bens, pessoas, serviços.

Conforme se depreende do caso analisado no capítulo 2, a promulgação da LGPD não partiu de uma negociação entre Brasil e UE (ou algum país Europeu), não houve a celebração de um tratado e a consequente incorporação de uma norma de proteção de dados pessoais. Na realidade, a promulgação da LGPD se deu a partir de complexos movimentos impulsionados mais indiretamente, a partir do levantamento de uma agenda de proteção de dados pessoais pela UE, da promulgação de uma norma por este ente cujo texto já previa responsabilidades para terceiros que, formalmente, não estão sujeitos a seu ordenamento jurídico e das repercussões desse debate em nível local, com a participação de diferentes setores da sociedade para além do Estado.

Esse dinamismo estimula a reformulação das teorias acerca da relação entre direito internacional e direito interno apontada acima, reconhecendo o desenvolvimento de um novo cenário jurídico que vislumbra as diferenças entre âmbito nacional e internacional, sem que haja prevalência ou mesmo negação de princípios comuns, interconexão e dependência de um quanto ao outro (ALVARADO, 2016, p. 33).

O autor Neil Walker (2008, p. 373) atribui ao intermeio desse novo cenário jurídico a expressão "desordem das ordens", na tentativa de explicitar que não há uma ordem dominante em uma nova configuração jurídica global, mas apenas tentativas de acomodação entre modelos e atores concorrentes, conforme trecho exposto a seguir):

> A recente proliferação de formas transnacionais de regulação e reconhecimento jurídico transformou a forma como entendemos a configuração jurídica global, tanto em termos quantitativos quanto qualitativos. (...) Em vez disso, há uma emergente "desordem das ordens", com discursividade tradicional estatal soberana, unipolar, de hierarquia global, regional, de campo jurídico (incluindo versões globais de direito "constitucional" e "administrativo"). grades de compreensão coerente e pluralista da relação entre ordens normativas que competem umas com as outras, mas sem que nenhuma ganhe ascendência. O futuro da configuração jurídica global provavelmente envolverá mais do mesmo. É provável que não presenciemos o restabelecimento de uma nova ordem dominante de ordens, mas, ao contrário, dependerá dos termos de acomodação alcançados entre esses modelos concorrentes e entre os atores – populares, judiciais e simbólicos – que são influentes em desenvolvê-los.[13] (WALKER, 2008, p. 373, tradução livre)

A diversidade de atores e poderes concorrentes sugerem a impossibilidade de existir um modelo pronto que seja capaz de definir qual o caminho de difusão percorrido por normas de caráter transnacional desde um âmbito global até o local e vice-versa. Pelo contrário, entende-se que cada temática ou norma possui diferentes contextos, meandros e peculiaridades que devem ser analisadas de acordo com o caso concreto.

---

[13] No original, "The recent proliferation of transnational forms of legal regulation and recognition has transformed the way we understand the global legal configuration, both in quantitative and in qualitative terms. (...) Rather, there is an emerging "disorder of orders," with traditional state sovereigntist, unipolar, global-hierarchy, regional, legal-field discursive (including global versions of both "constitutional" and "administrative" law), coherentist, and pluralist grids of understanding of the relationship between normative orders vying with one another, but with none gaining ascendancy. The future of the global legal configuration is likely to involve more of the same. It is likely we will not witness the reestablishment of a new dominant order of orders but, instead, will depend on the terms of accommodation reached among these competing models and among the actors— popular, judicial, and symbolic—who are influential in developing them."

Isso porque a perspectiva transnacional de difusão de normas não assume uma relação entre direito nacional e direito internacional de forma “automática”, e sim faz parte de um processo dinâmico, integrado por relações de poder e diferentes atores, conforme expõe Susanne Zwingel (2012, p. 116):

> A perspectiva transnacional — que considero mais abrangente — não pressupõe uma relação causal entre normas internacionais e domésticas. Em vez disso, conceitua a criação e apropriação de normas globais como um processo aberto de negociação no qual vários atores estão envolvidos. Todos esses atores são considerados contextualizados – não há diferença qualitativa entre local, nacional ou internacional – e vistos como parte de uma dinâmica não linear de produção normativa.[14] (ZWINGEL, 2012, p. 116, tradução livre)

Ressalta-se que essa perspectiva não busca desconsiderar a importância do Estado – é claro que, até mesmo formalmente, o Estado exerce relevantíssimo papel nas dinâmicas internacionais e as capacita nacionalmente, possuindo inclusive o poder para fazê-las cumprir a nível nacional -, contudo reconhece as evidências de que há uma formatação internacional que vão além dos modelos e visões tradicionais.

Reconhecer a existência dessa “desordem das ordens” é útil também para que sejam trazidos à tona os perigos relacionados a esse mundo globalizado e à transferência ou difusão internacional de normas, tais como às restrições à autodeterminação desses Estados, as limitações eventualmente impostas à democracia (PERJU, 2012, p. 2) e a adesão à modelos impulsionados por países com características econômicas e sociais profundamente divergentes, a fim de haver uma “adequação” ou “encaixe” a um ordenamento global (no qual, em muitos casos, países do Norte são exportadores, enquanto os do Sul são importadores) (OLIVEIRA; SARAIVA; SAKAI, 2020, p. 47). Questionamentos esses que, por si só, podem ser potencialmente aprofundados em outro estudo.

[14] No original, “The transnational perspective — which I consider more comprehensive— does not assume a causal relationship between international and domestic norms. Rather, it conceptualizes global norm creation and appropriation as an open process of negotiation in which various actors are involved. All these actors are considered contextualized—there is no qualitative difference between local, national, or international—and seen as being part of a nonlinear dynamic of norm production.”

5 CONSIDERAÇÕES FINAIS

O presente estudo foi realizado como trabalho de conclusão do Programa de Mestrado Profissional de Governanças Públicas e Formulação de Políticas Internacionais, tendo como objetivo aliar o conhecimento da academia com aspectos práticos de seus conceitos à realidade social, econômica e política.

A análise da difusão de normas, especialmente com o estudo do caso de transferência das regulamentações de dados pessoais, foi utilizada para alcançar esse objetivo. A análise do estudo foi realizada sob a perspectiva da teoria do “Efeito Bruxelas” da autora Anu Bradford (2020, p. 15), a qual explica a habilidade de a UE de penetrar a vida econômica de outras localidades a partir da exportação de normas, que é facilitada por mercados e empresas privadas.

Assim, utilizaram-se os elementos “de facto” (o qual observa o modo com que empresas e outros autores convergem à adoção da regulamentação europeia) e “de jure” (o qual explora como como governos não pertencentes à UE adotam domesticamente regulamentações similares) que integram a teoria (BRADFORD, 2020, p. 19) para condução da análise.

Como resultados, depreendeu-se que, no âmbito da perspectiva “de facto” – investigada a partir da exploração de documentos oficiais e outros materiais pertencentes ao histórico do processo legislativo da LGPD –, há evidências da atuação do setor privado na aprovação da LGPD, bem como do papel de impulsionador da EU.

Já no âmbito da perspectiva “de jure” – investigada a partir de uma análise comparativa do teor do RGPD e da LGPD –, entendeu-se que a LGPD tem extensas semelhanças com o RGPD, refletindo a intenção de harmonização nacional quanto ao referido normativo da UE, ainda que tenha contado com adaptações e adequações culturais, econômicas, linguísticas e qualitativas.

Assim, o estudo explorou de forma prática dinâmicas de influência, persuasão e negociação que permeiam o cotidiano da adoção de normas em um mundo globalizado e capitalista, aproximando as literaturas do Direito e das Relações Internacionais com o objetivo de empregar uma visão holística e contextualizada sobre essas dinâmicas.

Isso porque há um ponto de convergência entre Relações Internacionais e Direito, áreas que são interessadas no estudo das relações sociais como fenômenos

dinâmicos e em constante evolução (ZWINGEL, 2015, p. 115; LEGRAND, 2014, p. 29).

Nesse sentido, a literatura das Relações Internacionais interessa-se pela forma com a qual políticas públicas transferem-se, difundem-se e circulam internacionalmente, investigando o papel de diferentes atores da Governança Global nesse movimento (OLIVEIRA, 2017; ZWINGEL, 2012; SASSEN, 2015; BRADFORD, 2020). A autora Saskia Sassen (2015, p. 154-173) ressalta que esse movimento é reflexo de uma disputa de poderes em constante transformação, contando com o setor privado dentre os atores em disputa.

A literatura jurídica, por sua vez, dá especial atenção a esse movimento por meio do campo do direito comparado, chamando de “migrações”, “empréstimo” ou “transplante” de normas, conforme defendido por cada autor ou exposto em cada teoria, o movimento de uma norma em determinada ordem jurídica ser voluntariamente adotada em outra (PERJU, 2012; LEGRAND, 2014; CHOUDHRY, 2016). Há ainda aqueles autores que tratam do tema para exemplificar as rupturas que esses movimentos representam para as teorias tradicionais que buscam explicar o sistema internacional, em especial aquelas relacionadas à teoria monista e dualista fundamentados na Paz de Vestfália (ALVARADO, 2016, p. 33), como visto acima.

Unindo essas visões, este trabalho identificou que a promulgação da LGPD se deu a partir de complexos movimentos impulsionados pelo levantamento de uma agenda de proteção de dados pessoais pela EU. Esses movimentos geraram repercussões em nível local, com a participação de diferentes setores da sociedade para além do Estado, em especial o setor privado.

Assim, sem desconsiderar a importância do Estado no cenário internacional, entendeu-se que há uma formatação internacional que vai além dos modelos e visões tradicionais e que conta com uma diversidade de atores e poderes concorrentes, bem princípios comuns, interconexão e dependência, que sugerem a impossibilidade de existir um modelo pronto que seja capaz de definir qual o caminho de difusão percorrido por normas de caráter transnacional desde um âmbito global até o local e vice-versa.

Este trabalho propõe, portanto, que o estudo de cada temática ou norma deve ser analisado com atenção aos diferentes contextos, meandros e peculiaridades pertencentes a cada caso concreto, vez que há uma desordem na nova configuração

jurídica global e a constante tentativa de acomodação entre modelos e atores concorrentes.

Por fim, ressalta-se que o reconhecimento da existência dessa nova configuração, que foi objeto deste estudo, abre espaço para que sejam futuramente estudados os perigos relacionados a esse mundo globalizado e à transferência ou difusão internacional de normas, vez que podem implicar em restrições à autodeterminação de Estados, limitações à democracia e uma “adequação” forçada à critérios considerados adequados pelos atores dominantes dessa nova configuração global.

REFERÊNCIAS

ABRANET. **Manifesto sobre a Futura Lei de Proteção de Dados Pessoais**. Set. 2016. Disponível em: https://www.abranet.org.br/doc/manifesto_protecaodadospessoais.pdf?UserActiveTemplate=site. Acesso em: mai. 2022.

ACIOLLY, CASELLA e SILVA. **Manual de Direito Internacional Público**. 20ª ed. São Paulo: Editora Saraiva, 2012.

ALVARADO, Paula A. Zombis vs. Frankenstein: sobre las relaciones entre el derecho internacional y derecho interno. **Estudios Constitucionales**, Santiago, v. 14, nº 1, p. 15-60, jul. 2016.

ALVAREZ, José E. Are Corporations "subjects" of international law? **Santa Clara Journal of International Law**, v. 9, p. 32, 2011.

ALVES, Fabrício da Mota Alves. Entrevista concedida ao Observatório por DataPrivacyBR. Memória da LGPD – Observatório PPD, out-dez. 2019, episódio 3, item 4. Disponível em: https://www.observatorioprivacidade.com.br/memoria/2018-uma-conjuncao-astral/. Acesso em: mai. 2022.

APPLE. **App Store Review Guidelines**. 30 de março de 2022. Disponível em: https://developer.apple.com/app-store/review/guidelines/#5.1.1. Acesso em: abr. 2022.

BECKER, Tilman. Big Data Usage. In: CAVANILLAS, José María; CURRY, Edward; WAHLSTER, Wolfgang (Eds.). **New Horizons for a Data-Driven Economy**. Switzerland: Springer International Publishing, 2016.

BRAITHWAITE, Alex; JEONG, Sangmi. Diffusion in International Politics. **Oxford Research Encyclopedia of Politics**, Oxford University Press, 28 june 2017.

BRADFORD, Anu. **The Brussels Effect: how the European Union rules the world**. New York: Oxford University Press, 2020.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4060/2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências**. NOVA EMENTA: Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Brasília: Câmara dos Deputados, 2012. Disponível em: https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-4060-2012. Acesso em: fev. 2022.

BRASIL. **Código Civil Brasileiro, 2002**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: dez. 2020.

BRASIL. **Constituição Federal, 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: dez. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: jun. 2020.

BRASSCOM**. Manifesto pela Aprovação da Lei de Proteção de Dados Pessoais**. Jul. 2018. Disponível em: https://brasscom.org.br/pdfs/manifesto-pela-aprovacao-da-lei-de-protecao-de-dados-pessoais/. Acesso em: mai. 2022.

CAVANILLAS, José María; CURRY, Edward; WAHLSTER, Wolfgang (Eds.). **New Horizons for a Data-Driven Economy**. Switzerland: Springer International Publishing, 2016.

CHANG, Wen-Chen; YEH, Jiun Rong. Internationalization of Costitutional Law. In: ROSENFELD, M.; SAJÓ, A. **The Oxford Handbook of Comparative Constitutional Law**. Estados Unidos: Oxford University Press, 2012.

CHANG, Wen-Chen; YEH, Jiunn-Rong. Internationalization of Constitutional Law. In: ROSENFELD, M.; SAJÓ, A. **The Oxford Handbook of Comparative Constitutional Law**. Estados Unidos: Oxford University Press, 2012.

CHOUDHRY, S. **The Migration of Constitutional Ideas**. Nova Iorque: Cambridge University Press, 2006.

CHOW, Beatriz G.; LIMA, Clarisse L. F. Data protection implications through an inner-connected world: European Union's contributions towards the brazilian legislative scenario. **Latin American journal of European Studies**, vol. 01, nº 01 - jan/june 2021.

CLARKE, Roger. Direct Marketing and Privacy. **Roger Clarke's Web-Site**, Xamax Consultancy Pty Ltd, 23 feb. 1998. Disponível em: http://www.rogerclarke.com/DV/DirectMkting.html. Acesso em: jun. 2021.

DATA PRIVACY BRASIL. Tudo o que você precisa saber sobre as tecnologias de rastreamento utilizadas no combate à COVID-19. **Observatório Privacidade**, 21 set. 2020. Disponível em: https://observatorioprivacidade.com.br/2020/09/21/tudo-o-que-voce-precisa-saber-sobre-as-tecnologias-de-rastreamento-utilizadas-no-combate-a-covid-19/. Acesso em: 04 dez. 2020.

DATAPRIVACYBR. **Memória da LGPD**. Observatório Privacidade. Disponível em: https://www.observatorioprivacidade.com.br/memorias/. Acesso em: mai. 2022.

DOLOWITZ, D.; MARSH, D. Learning from abroad: the role of policy transfer in contemporary policy making. **Governance**, 13(1), p. 5–24, 2000.

DOLOWITZ, D.; MARSH, D. Who learns from whom: a review of the policy transfer literature. **Political Studies**, 44(2), p. 343–57, 1996.

EUA. Estados Unidos da América. **California Consumer Privacy Act of 2018**. California Law – Civil Code, 2018. Disponível em:

http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. Acesso em: dez. 2020.

EUA. Estados Unidos da América. **Stop Hacks and Improve Electronic Data Security Act**. New York, 2020. Disponível em: https://www.nysenate.gov/legislation/bills/2019/S5575. Acesso em: dez. 2020.

GALLINDO, Sergio Paulo. Entrevista concedida ao Observatório por DataPrivacyBR. Memória da LGPD – Observatório PPD, out-dez. 2019, episódio 2, item 11. Disponível em: https://www.observatorioprivacidade.com.br/memoria/2016-2017-o-anteprojeto-chega-a-camara/. Acesso em: mai. 2022.

GUTIERREZ, Andriei. Relações Governamentais sobre Temas Transnacionais: o caso da LGPD. Entrevista concedida ao Projeto Estuário – PUC-SP. 2020. Disponível em: https://www.youtube.com/watch?v=JNxP6E0HD-s&t. Acesso em: mai. 2022.

IDEC. **Posicionamento sobre os Projetos de Lei 5.276/16 e 4.060/12 apresentado à Comissão Especial de Tratamento e Proteção de Dados Pessoais da Câmara dos Deputados**. Dez. 2016. Disponível em: http://www.idec.org.br/ckfinder/userfiles/files/Posic_a_o%20do%20Idec_Dezembro%20de%202016.pdf. Acesso em: abr. 2022.

JAPÃO. APPI. Amended Act on the Protection of Personal Information. Personal Information Protection Commission, Dec. 2016. Disponível em: https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf. Acesso em: dez. 2020.

KELSEN, Hans. **Les rapports de système entre le droit interne et le droit internacional public**. Paris: Recueil des Cours, Académie de Droit International, 1926.

LEGRAND, Pierre. A Impossibilidade de “Transplantes Jurídicos”. **Cadernos do Programa de Pós-Graduação em Direito**, UFRGS, vol. IX, n. 1, 2014.

LESSA, Rafaela; REIS, Daniela M. A ONU e a responsabilidade internacional de empresas por transgressão aos direitos humanos. **RIDH**, Bauru, v. 5, n. 2, jul./dez., p. 261-274, 2017.

LGPD ACADÊMICO. YUN, Remilina (Coord.). LGPD Acadêmico – Comparativo. **LGPD Acadêmico – Creative Common**, v. 1, 17 fev. 2020. Disponível em: https://www.lgpdacademicooficial.com.br/_files/ugd/c4fd4b_f3e0d4ccbbbe40a0a51ec82e993af11c.pdf. Acesso em: fev. 2022.

LIVINGSTON, Steven G. The Politics of International Agenda-Setting: Reagan and North-South. **International Studies Quarterly**, Vol. 36, No. 3, Sep. 1992, p. 313-329.

META. **Política de Dados**. 4 de janeiro de 2022. Disponível em: https://www.facebook.com/about/privacy/update. Acesso em: abr. 2022.

MICHAELS, Daniel. Hot U.S. Import: European Regulations. **Wall St. Journal**, 7 mai. 2018. Disponível em: https://www.wsj.com/articles/techs-pickup-of-new-data-privacy-rules-reflects-eus-growing-influence-1525685400. Acesso em: jan. 2022.

MONTEIRO, Carina. Direito à privacidade versus direito à informação. **Revista de informação legislativa**, Vol. 44, n. 173, jan.-mar. 2007, p. 27-40.

NELKEN, D. Comparatists and Transferability. In: LEGRAND, P.; MUNDAY, R. (Eds.). **Comparative Legal Studies: Traditions and Transitions**. Cambridge: Cambridge University Press, 2003, p. 437 - 442.

NEWMAN, Abraham; BACH, David. The European Union as hardening agent: soft law and the diffusion of global financial regulation. **Journal of European Public Policy**, Vol. 21, No. 3, p. 430 - 452, 2014.

OEA. **Declaração Americana dos Direitos e Deveres do Homem, 1948**. Disponível em: https://www.cidh.oas.org/basicos/portugues/b.declaracao_americana.htm. Acesso em: dez. 2020.

OLIVEIRA, Osmany Porto De; SARAIVA, Camila; SAKAI, Roberta. **Difusão de Políticas e Cooperação para o Desenvolvimento: elementos norteadores para a implementação de projetos de transferência de políticas públicas por meio da cooperação internacional**. São José do Rio Preto, SP: Balão Editorial, 2020.

OLIVEIRA, Osmany. **International Policy Diffusion and Participatory Budgeting**. Palgrave Macmilan, 2017.

ONETRUST DATAGUIDANCE; BAPTISTA LUZ ADVOGADOS. **Comparing Privacy Laws: RGPD v. LGPD. 2019.** Disponível em: https://baptistaluz.com.br/comparing-privacy-laws-RGPD-v-lgpd/. Acesso em: fev. 2022.

ONU. **Declaração Universal dos Direitos do Homem, 1948**. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: dez. 2020.

PARLAMENTO EUROPEU. As Fontes e o Âmbito de Aplicação do Direito da União Europeia. Fichas Técnicas sobre a União Europeia, 2022. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_1.2.1.pdf. Acesso em: jun 2022.

PERJU, Vlad. Constitutional Transplants, Borrowing, and Migrations. In: ROSENFELD, M.; SAJÓ, A. **The Oxford Handbook of Comparative Constitutional Law**. Estados Unidos: Oxford University Press, 2012.

PINHEIRO, Patricia Peck. Nova Lei Brasileira de Proteção de Dados Pessoais (LGPD) e o Impacto nas Instituiçoes Públicas e Privadas. **Revista Eletrônica: Lei Geral de Proteção de Dados**, Tribunal Regional do Trabalho da 9ª Regiao, vol. 10, n. 97, p. 75-87, mar. 21. Disponível em: https://juslaboris-hml.tst.jus.br/bitstream/handle/20.500.12178/185970/2021_rev_trt09_eletr_v0010_n0097.pdf?sequence=1&isAllowed=y. Acesso em: jul. 2022.

PIOVESAN, Flávia Cristina; GONZAGA, Victoriana. Empresas e direitos humanos: desafios e perspectivas à luz do direito internacional dos direitos humanos. **R. Trib. Reg. Fed. 1ª Região**, Brasília, DF, v. 31, nº 1, 2019.

PORNWASIN, Asina. Thai Data Protection Laws Must Quickly be Updated to EU Standards. **The Nation**, 25 mai. 2018. Disponível em: http://www.nationmultimedia.com/detail/national/30346209. Acesso em: jan. 2022.

ROSEN, Jeffrey. Why privacy matters. **The Wilson Quarterly**, Vol. 24, No. 4, Outono 2000, p. 32-38.

ROSENAU, James. **Along the Domestic-Foreign Frontier: Exploring Governance in a Turbulent World**. Washington DC: Cambridge University Press, 1997.

SÁNCHEZ-BAYÓN, Antonio. **Sistema de Derecho Comparado y Global: de las famílias jurídicas mundiales al nuevo derecho común**. Valencia: Tirant lo blanc, 2012.

SASSEN, Saskia. Neither global nor national: Novel assemblages of territory, authority, and rights. **Global Crises and the Challenges of the 21st Century: Antisystemic Movements and the Transformation of the World-System**, v. 4951, 2015. p. 154 - 173.

SCOTT, Mark Scott; CERULUS, Laurens. Europe's New Data Protection Rules Export Privacy Standards Worldwide. **Politico**, 31 jan. 2018. Disponível em: https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/. Acesso em: jan. 2022.

SOLOVE, Daniel J. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. **San Diego Law Review**, Vol. 44, No. 289, 2007, p. 745.

STONE, Diane. Transfer agents and global networks in the 'transnationalization' of policy. **Journal of European Public Policy**, 11:3, p. 545-566, jun. 2004.

TOMASEVICIUS, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Instituto de Estudos Avançados - USP**, vol. 30 (86), 2016.

TORRES, Raquel. O Congresso vai decidir sobre seus dados pessoais. **Outras Palavras**, Especiais, 08 mai. 2019. Disponível em: https://outraspalavras.net/outrasaude/o-congresso-vai-decidir-sobre-seus-dados-pessoais/. Acesso em: abr. 2022.

TRIEPEL, Carl Heinrich. Les rapports entre le droit interne et le droit international. **RCADI**, t. 1, p. 73-122, 1923.

UE. União Europeia. **Carta dos Direitos Fundamentais da União Europeia**, de 18 de dezembro de 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: set. 2021.

UE. União Europeia. **Diretiva Europeia de Proteção de Dados**, de 24 de outubro de 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: set. 2021.

UE. União Europeia. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: set. 2020.

WALKER, Neil. Beyond boundary disputes and basic grids: Mapping the global disorder of normative orders, **International Journal of Constitutional Law**, Vol. 6, Issue 3-4, July-October 2008, p. 373–396.

WATSON, Alan. **Legal Transplants: An Approach to Comparative Law**. Athens: The University of Georgia Press, 1993.

ZANATTA, Rafael. Entrevista concedida ao Observatório por DataPrivacyBR. Memória da LGPD – Observatório PPD, out-dez. 2019, episódio 1, item 7. Disponível em: https://www.observatorioprivacidade.com.br/memoria/2010-2015-o-tema-entra-em-pauta/. Acesso em: mai. 2022.

ZWINGEL, Susanne. How Do Norms Travel? Theorizing International Women's Rights in Transnational Perspective. **International Studies Quarterly**, vol. 56, no. 1, 2012, p. 115–129.

ANEXO A – Manifesto sobre a Futura Lei de Proteção de Dados Pessoais

MANIFESTO SOBRE A FUTURA LEI DE PROTEÇÃO DE DADOS PESSOAIS

SETEMBRO DE 2016

É inquestionável o papel que a Internet tem na sociedade como viabilizadora de inclusão social, indutora de crescimento econômico, inovação e avanço tecnológico. Especialistas preveem que o tratamento e a monetização de dados gerarão cerca de US$ 1,6 trilhão de valor agregado nos próximos quatro anos.

Neste contexto, a proteção de dados pessoais é um dos grandes desafios da atualidade. O Brasil tem a oportunidade de conceber uma Lei de Proteção de Dados Pessoais moderna e balanceada, que proteja os direitos do cidadão e que seja impulsionadora do desenvolvimento tecnológico e de modelos de negócios inovadores.

As entidades que subscrevem este manifesto entendem que a futura lei de proteção de dados pessoais deve contemplar os aspectos detalhados a seguir.

DADO PESSOAL

Devem ficar sujeitos à lei somente os dados que inequivocamente possam ser utilizados para identificar a pessoa natural, podendo assim afetar a sua privacidade, devendo ser excluídos desta definição todos os demais.

Um conceito amplo de dado pessoal pode inibir o desenvolvimento da economia e inovação baseada em dados, na medida em que os tratamentos englobam dados que são meramente relacionados a pessoas naturais ou identificação eventual quando combinados com outros dados pessoais. Uma conceituação ampla tornaria praticamente todos os dados produzidos pela atividade humana sujeitos à Lei, ainda que não possam ser utilizados para identificar inequivocamente o titular.

Recomenda-se a seguinte definição de **dado pessoal: qualquer dado que identifique de forma exata e precisa uma pessoa natural**.

DADOS PESSOAIS SENSÍVEIS

Recomenda-se que seja adotada uma definição de dados sensíveis taxativa, evitando-se definições abertas e genéricas, a exemplo do que se dá em outros países, em razão de sua especialidade e das diversas restrições impostas à sua coleta e tratamento.

Em geral, não se configuram como dados de saúde os dados gerados por aplicativos de estilo de vida e dispositivos medidores, não requerendo, portanto, proteção especial. Por outro lado, direito à manifestação pública a respeito de convicções religiosas, opiniões políticas, ou filiação a sindicatos não deve ser cerceado. Assim sendo a futura lei de proteção de dados deve reconhecer e respeitar a expressão de tais convicções ou filiações, quando forem espontânea e livremente fornecidas pelos titulares, como manifestação de pensamento, consciência ou crença, e que constituem a base da liberdade de expressão e do exercício pleno da cidadania.

Portanto, recomenda-se a seguinte definição de **dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados médicos, genéticos e referentes à orientação afetiva e de gênero.**

Neste sentido, recomenda-se que o tratamento de dados pessoais sensíveis, voluntariamente disponibilizados por seus titulares, prescinda de consentimento diferenciado, como se segue: **Os dados pessoais sensíveis que sejam voluntariamente disponibilizados por seus titulares como manifestação de sua liberdade de expressão, consciência ou crença, poderão ser tratados como dados pessoais**.

DADOS ANÔNIMOS

Os dados não relacionados a uma pessoa natural específica são a espinha dorsal do modelo da economia impulsionada por dados, que hoje representa um acelerador do desenvolvimento econômico e da inovação tecnológica. Não devem estar sujeitas à aplicação da Lei dados pessoais que tenham sido anonimizados ou que de qualquer outra forma não possam identificar a pessoa natural. Recomenda-se a seguinte definição de **dados anônimos: dados relativos a um titular que não seja identificado**.

CONSENTIMENTO

A adoção do consentimento livre e inequívoco, em oposição ao consentimento expresso estabelecido em outros diplomas legais, viabiliza o tratamento de dados no ambiente digital conectado, permite a contínua inovação baseada em dados e assegura o nível de proteção adequado ao titular.

O **consentimento inequívoco**, inserido como regra geral para a manifestação do consentimento, é entendido como **uma declaração do titular** que visa a proteger seus direitos e se compatibiliza com o dinamismo da era da Internet, podendo ser **expressa por escrito**, **por meios eletrônicos**, **declarações orais**, **configurações técnicas** para o processamento de dados e informações pessoais, **ou qualquer outra forma** de expressar a aceitação do titular quanto ao processamento e tratamento dos seus dados pessoais.

Ressalte-se a necessidade de harmonizar a Lei 12.965/2014, Marco Civil da Internet, às disposições da futura Lei de Proteção de Dados Pessoais.

DO INTERESSE LEGÍTIMO

O reconhecimento do legitimo interesse implica em que dados podem ser regularmente tratados, sem a necessidade de obtenção de consentimento, sempre que o responsável tiver interesse em tal tratamento, mediante balanceamento com os interesses, direitos e liberdades fundamentais do titular dos dados e a necessidade do tratamento do dado.

A importância do interesse legítimo é evidenciada ante a constatação de que o conceito tradicional de consentimento não lida adequamente com o tratamento de dados em larga escala ("big data") e com o cenário de novos dispositivos conectados.

RESPONSABILIDADE CIVIL

A responsabilização das empresas que tratam dados e prestam serviço ao usuário em relação aos dados pessoais deve se dar no tocante (i) ao respeito aos **direitos e liberdades fundamentais** do titular, (ii) ao **tratamento dos dados** no âmbito do consentimento, do legítimo interesse, ou nas demais hipóteses previstas em lei, e (iii) ao **dever de guarda** dos dados tratados.

No caso de descumprimento de seus deveres, **a empresa que** tratou os dados responderá **pelos danos causados** ao titular dos dados estritamente no âmbito de sua atuação dentro da cadeia de tratamento, devendo ser apuradas as respectivas responsabilidades de cada uma das demais empresas especializadas por ela contratadas.

Por sua vez, a responsabilização das empresas subcontratadas na cadeia de tratamento deve se dar no tocante (i) aos **termos e condições pelos quais foram contratadas** e (ii) ao **dever de guarda** dos dados a serem tratados e os respectivos resultados do tratamento, **sem a necessidade de regulação *ex ante*** por parte de eventual Órgão Competente.

Veja-se que, por serem pessoas jurídicas diversas e independentes, as empresas não poderão exercer controle sobre as atividades umas das outras e, portanto, não é razoável atribuir-se responsabilidade solidária entre elas por atos sobre os quais não tem poder de supervisão que lhes permita controlar e evitar os prejuízos que serão obrigadas a reparar. Convém citar o exemplo do Cadastro Positivo, em que a responsabilidade objetiva e solidária entre fontes, consulentes e bancos de dados, tem representado um importante entrave para a implementação exatamente em razão do argumento acima exposto.

Ressalte-se que as empresas que compõem a cadeia de empresas subcontratadas pela empresa que trata os dados e presta serviço para o usuário, podem estar no Brasil ou em qualquer outro lugar do mundo.

Sugere-se, portanto, que as empresas cedentes (empresas que coletam dados e prestam serviço ao usuário) e cessionárias (empresas subcontratadas na cadeia de tratamento) respondam dentro dos limites de sua atuação pelos danos decorrentes na cadeia de tratamento de dados, independentemente do local onde estes se localizem, devendo ser apuradas as respectivas responsabilidades, cabendo (i) ao cedente, a responsabilidade pela integridade dos dados pessoais transmitidos tais como coletados e pela comunicação de eventuais alterações nos dados ou no consentimento ao cessionário; (ii) ao cessionário, a integridade dos dados pessoais tais como transmitidos pelo cedente, pelo seu tratamento em conformidade com as hipóteses legais e pela integridade dos dados de acordo com posteriores comunicações do cedente.

TRANSFERÊNCIA INTERNACIONAL DE DADOS

O fluxo internacional de informações é uma importante fonte de valor econômico e social, sendo que um dos grandes benefícios da sociedade digital está justamente nas economias de escala advindas desse ecossistema. A experiência recente demonstra que as medidas adotadas pelas empresas para garantir a segurança da transferência internacional de dados são tão ou mais eficazes para proteger os dados e bem mais ágeis no acompanhamento da inovação tecnológica, do que sistemas regulatórios baseados na avaliação *ex ante* da adequação de sistemas regulatórios estrangeiros. **Assim, as empresas são incumbidas por zelar pela integridade dos dados e serão responsabilizadas caso ocorra a transferência para empresas que não adotem política de proteção adequada**, **sem a necessidade de regulação *ex ante*** por parte de um Órgão Competente.

ÓRGÃO REGULADOR INDEPENDENTE

É fundamental a criação de uma autoridade federal independente para interpretar, fiscalizar e fazer cumprir a futura norma sobre proteção de dados pessoais. Internacionalmente, quase todos os países que promulgaram leis de proteção de dados pessoais criaram um órgão nacional específico e independente com essas competências.

As vantagens de um modelo de autoridade federal independente estão na consistência das interpretações, a especialização técnico-jurídica sobre o tema, a certeza regulatória e a independência necessária para atuar de modo eficaz e sopesar todos os direitos e interesses em jogo. Ressalve-se, porém, que o orçamento operacional do órgão deve ser autônomo, sem incluir eventuais multas impostas em decorrência de violações à lei, pois do contrário haveria um claro conflito de interesses e incentivo a distorções.

SANÇÕES E PROPORCIONALIDADE

As sanções previstas na futura lei devem ser proporcionais à natureza das violações de direito e dos danos efetivamente causados. Sanções que suspendem ou proíbem o tratamento de dados, ainda que por tempo determinado, podem acarretar o encerramento de atividades empresariais, abrindo espaço para possível violação dos direitos fundamentais dos titulares, como liberdade de expressão e comunicação, representando um forte fator de insegurança jurídica e de desestímulo a investimentos e à prestação de serviços no Brasil.

VACATIO LEGIS

Em razão da complexidade do seu objeto, leis de proteção de dados afetam de forma ampla (a) o setor privado, que se adapta às novas regras, (b) a Administração Pública, que se organiza para desempenhar novas funções, e (c) o poder judiciário, que empreende a exegese da lei. A experiência Internacional, em especial a Europeia, demonstra que se faz mister um período de transição e adaptação, tendo em vista o novidadismo. Assim sendo, sugere-**se que a futura lei entre em vigor após 3 (três) anos, contados a partir da data da sua sanção**.

LEGITIMIDADE DA COLETA E TRATAMENTO ANTERIORES À LEI

O direito brasileiro adota como regra geral a irretroatividade dos efeitos da nova lei, protegendo o ato jurídico perfeito. Os novos requisitos a serem trazidos pela futura lei não invalidam os dados coletados e tratados sob a égide da legislação vigente à época. Condiciona-se, porém, novos tratamentos, bem como os direitos de acesso e retificação, ao disposto na futura lei. Sugere-se, portanto, que **os dados pessoais armazenados pelos responsáveis em conformidade com a legislação vigente à época de sua coleta não estarão sujeitos à obtenção do consentimento dos seus titulares, aplicando-se às subsequentes operações de seu tratamento, contudo, as demais disposições desta lei**.

ANEXO B - Manifesto pela Aprovação da Lei de Proteção de Dados Pessoais

MANIFESTO PELA APROVAÇÃO DA LEI DE PROTEÇÃO DE DADOS PESSOAIS

Em defesa da aprovação, pelo Senado, do Projeto de Lei da Câmara nº 53 de 2018

São Paulo, 26 de junho de 2018

As entidades representativas, instituições acadêmicas, organizações e pessoas que subscrevem este documento, manifestam apoio à **célere apreciação e aprovação**, por parte do Senado Federal, do **Projeto de Lei da Câmara dos Deputados nº 53/2018**, que dispõe sobre proteção de dados pessoais no Brasil.

Vários países já contam com regramentos de proteção de dados pessoais, endereçando os desafios da transformação social e da econômica decorrente do avanço da tecnologia digital, em reconhecimento ao enorme potencial de desenvolvimento bem-estar derivado da geração, coleta e tratamento de expressiva quantidade de dados. Uma **lei de proteção de dados clara** e **principiológica**, que **equilibre** a **posição central do indivíduo** com o **dinamismo econômico** de um país criativo e inclinado à inovação, como o Brasil, é essencial para catalisar competitividade.

Os debates empreendidos **nas duas casas do Congresso Nacional**, envolvendo **autoridades públicas** e representantes da **academia**, da **sociedade civil** e dos **setores empresariais**, intensificados nos dois últimos anos, **logrou conquistar exitosa convergência** e contribuíram para a composição do **texto recém aprovado** na Câmara de Deputados. Assim, entendemos que o PLC nº 53/2018 **atende a imperiosa necessidade segurança jurídica para cidadãos e agentes econômicos**. **O Senado tem oportunidade ímpar** de conferir **protagonismo ao Brasil**, em termos de legislação de dados, passo fundamental para a inserção do País em foros internacionais bem como, de **proporcionar um ambiente de negócios seguro** que potencialize a **atração e materialização de investimentos na ordem de R$ 250 bilhões** (Brasscom e Frost & Sullivam) em tecnologias de transformação digital até 2021.

O PLC nº 53/2018, ora sob a análise do Senado, é considerado pelos signatários deste manifesto, um **texto que está em sintonia com as melhores práticas internacionais**, **equilibrando a garantia dos direitos individuais** com a **indução de novos modelos de negócios intensivos em dados**. Ressalte-se, ainda, que o texto encampa a criação da **Autoridade Nacional de Proteção de Dados, independente funcional e financeiramente,** e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, **órgãos essenciais** para operacionalização do futuro diploma, corroborando iniciativa do Poder Executivo Federal quando da submissão do Projeto de Lei 5.276/2016.

A **futura Lei** de Proteção de Dados Pessoais alcançará as esferas **pública e privada**, bem como **setores econômicos** com atuação nos ambientes tradicional e digital conectado. O **texto** aprovado pela Câmara dos Deputados **legitima o tratamento de dados** realizado com **base em parâmetros e garantias** adequadas aos seus **titulares**, com **controle e transparência** sobre os processos de tratamento, assegurando **segurança jurídica e confiança** ao ecossistema envolvido.

Ante o exposto**, instamos o Senado Federal a apreciar a aprovar o PLC nº 53/2018 com máxima celeridade em prol do melhor interesse do Brasil!**

Subscrevem este Manifesto:

MANIFESTO PELA APROVAÇÃO DA LEI DE PROTEÇÃO DE DADOS PESSOAIS

Em defesa da aprovação, pelo Senado, do Projeto de Lei da Câmara nº 53 de 2018

São Paulo, 26 de junho de 2018

ABCD – Associação do Crédito Digital

ABERT – Associação Brasileira de Emissoras de Rádio e Televisão

ABES – Associação Brasileira das Empresas de Software

Assespro – Federação das Associações das Empresas Brasileiras de Tecnologia da Informação e Comunicação

Brasscom – Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação

Coalizão Direitos na Rede

- Actantes
- Articulação Marco Civil Já
- Artigo 19
- ASL — Associação Software Livre
- Casa da Cultura Digital de Porto Alegre
- Centro de Estudos da Mídia Alternativa Barão de Itararé
- Centro de Tecnologia e Sociedade da FGV-RJ
- Ciranda da Comunicação Compartilhada
- Coding Rights
- Colaboratório de Desenvolvimento e Participação — COLAB-USP
- Coletivo Digital
- Coolab - Laboratório Cooperativista de Tecnologias Comunitárias
- Garoa Hacker Clube

MANIFESTO PELA APROVAÇÃO DA LEI DE PROTEÇÃO DE DADOS PESSOAIS

Em defesa da aprovação, pelo Senado, do Projeto de Lei da Câmara nº 53 de 2018

São Paulo, 26 de junho de 2018

- Grupo de Estudos em Direito, Tecnologia e Inovação do Mackenzie
- Grupo de Pesquisa em Políticas Públicas para o Acesso a Informação/GPoPAI da USP
- Idec — Instituto Brasileiro de Defesa do Consumidor
- Instituto Alana
- Instituto Beta: Internet & Democracia
- Instituto Bem-Estar Brasil
- Intervozes — Coletivo Brasil de Comunicação Social
- Instituto Iris
- Instituto Igarapé
- Instituto Nupef
- ITS-Rio — Instituto de Tecnologia e Sociedade do Rio de Janeiro
- LAVITS — Rede latina-americana de estudos sobre vigilância, tecnologia e Sociedade
- Movimento Mega
- Núcleo de Estudos em Tecnologia e Sociedade da USP — NETS/USP
- PROTESTE — Associação de Consumidores
- Internet Sem Fronteiras Brasil

CACB – Confederação das Associações Comerciais e Empresariais do Brasil

CEDIS IDP – Centro de Direito, Internet e Sociedade do IDP, Instituto Brasiliense de Direito Público

Crypto ID – Portal de notícias sobre identificação digital e tecnologia

Danilo Doneda – Doutor em Direito Civil, Professor no Mestrado do IDP, Instituto Brasiliense de Direito Público

Fenainfo – Federação Nacional da Empresas de Informática

ITS-Rio – Instituto de Tecnologia e Sociedade do Rio de Janeiro

MBC – Movimento Brasil Competitivo

ANEXO C - Quadro comparativo de normas de proteção de dados pessoais

LGPD ACADÊMICO - COMPARATIVO

Categorias	Atividades de Gerenciamento de Privacidade e Proteção de Dados Pessoais	GDPR	LGPD	CCPA	PCI	BACEN 4658	ISO27001/27002	ISO27701
1. Manter estrutura de governança	Atribuir a responsabilidade pela privacidade e proteção dos dados a um indivíduo (por exemplo, Privacy Officer, Privacy Counsel, CPO, entre outros)	Art. 27	Art. 61	--	--	Art. 7	6.1.1	6.3.1.1
	Envolver o C-Level em privacidade e proteção de dados (por exemplo, no Conselho de Administração, Comitê Executivo)	--	--	--	--	Art. 9		
	Designar um encarregado de proteção de dados/DPO com uma função independente	Art. 37, 38	Art. 41	--	--	--	6.1.1	6.3.1.1
	Atribuir responsabilidade pela privacidade e proteção dos dados em toda a organização (por exemplo, Rede de Privacidade, Privacy Champions, etc)	Art. 24, §2º	Art. 50	--	--	--	6.1.1	
	Manter funções e responsabilidades dos responsáveis pela privacidade e proteção dos dados (por exemplo, descrições de cargo)	Art. 39	Art. 41, §2º	--	12	--	5.1,5.3; 6.1.1; 7.2.2	6.3.1.1,6.4.2.2
	Conduzir comunicação regular entre o privacy office, privacy network e outros responsáveis pela privacidade e proteção de dados	Art. 38	Art. 41, §2º	--	--	--		6.3.1.1
	Envolver todas as partes interessadas da organização em questões de privacidade e proteção de dados	--	--	--	--	Art. 4, 5	6.1.1,6.1.4	--
	Reportar às partes interessadas internas da organização o status do gerenciamento de privacidade e proteção de dados (por exemplo, conselho de administração, gerenciamento)	--	--	--	12	Art. 4	5.1.1	
	Reportar às partes interessadas externas da organização o status do gerenciamento de privacidade (por exemplo, órgãos reguladores, terceiros, clientes)	--	--	--	12	Art. 23	5.1.1	
	Realizar uma avaliação de risco de privacidade e proteção de dados da empresa	Art. 24, 39	Art. 50	--	--	Art. 2, §1; 11	4.1; 5.1.1, 18	5.2.1,6.2.1.1,6.3.1.1, 6.4.2.2, 6.15.1.3,7.2.8,
	Integrar a privacidade de dados nas avaliações / relatórios de risco corporativo	--	--	--	--	--	--	--
	Manter uma estratégia de privacidade e proteção de dados	--	--	--	--	--	--	--
	Manter um programa de privacidade e proteção de dados	--	--	--	--	--	--	--
	Exigir que os funcionários reconheçam e concordem em aderir às políticas de privacidade e proteção de dados	--	--	--	--	Art. 3, VI, a	7.1.2, 7.2.2,7.2.3	
2. Manter inventário de dados pessoais	Manter um inventário de dados pessoais que são tratadas (5W2H dos dados pessoas)	Art. 30	Art. 37	--	--	--	8.1.1	6.12.1.2, 7.5.2, 7.5.3,7.5.4, 8.2.6, 8.4.2, 8.5.2,8.5.3
	Classificar os dados pessoais tratado (por exemplo, secreto, confidencial, restrito, público)	--	--	--	--	Art. 3, V, c	8.2	
	Obter aprovação dos reguladores e/ou autoridades para processamento de dados (onde é necessária aprovação prévia)	--	--	--	--	--	--	--
	Registrar bancos de dados com reguladores e/ou autoridades (onde o registro é necessário)	--	--	--	--	--	--	--
	Manter fluxogramas dos fluxos de dados (por exemplo, entre sistemas, entre processos, entre países)	Art. 30	Art. 37	--	--	--	--	--
	Manter registros do mecanismo de transferência usado para fluxos de dados transfronteiriços (por exemplo, cláusulas contratuais padrão, regras corporativas vinculativas (BCR), aprovações de órgãos reguladores, se necessário, entre outros)	Art. 45, 46, 49	Art. 33	--	--	--	--	7.5.1,8.5.1
	Adotar Regras Corporativas Vinculativas (BCR - Binding Corporate Rules) como um mecanismo de transferência de dados	Art. 46, 47	Art. 33	--	--	--	--	7.5.1,8.5.1
	Adotar contratos como um mecanismo de transferência de dados (por exemplo, cláusulas contratuais padrão)	Art. 46	Art. 33	--	--	--	13.2	7.5.1, 8.5.1
	Adotar regras de privacidade e proteção de dados nas transferência de dados	--	--	--	--	--	--	
	Obter a aprovação do regulador e/ou autoridade para transferência de dados	Art. 46	Art. 33, 36	--	--	--	--	7.5.1,8.5.1
	Adotar uma das bases legais para transferência de dados	Art. 45, 48, 49	Art. 33	--	--	--	--	7.5.1,8.5.1,8.5.5
	Manter EU-US Privacy Shield como um mecanismo de transferência de dados	Art. 46	--	--	--	--	--	7.5.1,8.5.1
3. Manter a política de privacidade e proteção de dados	Manter uma política de privacidade e proteção de dados	Art. 5, 24, 91	Art. 6, 14, 15, 50	1798.135 (a) (2)	1,2,3,4,5,6, 7,8,9,10, 11, 12	Art. 2	5.1, 6.1.2, 6.2, 8.2.1, 8.2.2, 8.3.1, 8.3.2, 8.3.3, 9.2.1,9.2.2, 9.4.2, 10, 11.2.7,11.2.9,12.3.1,12.4.1, 12.4.2,13.2.1, 13.2.4,14.1.2,14.3.1,15.1.2, 16.1.1,18.1.1,18.1.3,	5.2.1,6.2.1.1, 6.3.2.1, 6.5.2.1,6.5.2.2, 6.5.3.1,6.5.3.2,6.5.3.3,6.6.2.1,6.6.2.2,6.6.4.2, 6.8.2.7, 6.8.2.9, 6.9.3.1,6.9.4.1, 6.9.4.2, 6.10.2.1, 6.10.2.4, 6.11.1.2, 6.11,3,1,6.12.1.2,6.13.1.1, 6.15.1.1, 6.15.1.3, 7.2.1, 7.2.2, 7.2.8,7.3.6,7.4.1, 7.4.3, 7.4.4, 7.4.5, 7.4.6, 7.4.8, 7.4.9, 8.2.2, 8.4.1, 8.4.3,
	Manter uma política de privacidade e proteção de dados de funcionários	--	--	--	--	--	--	--
	Documentar a base legal para o tratamento de dados pessoais	Art. 6, 9, 10	Art. 7, 10, 11,14	--	--	--	--	--
	Integrar ética ao tratamento de dados (códigos de conduta, políticas e outras medidas)	Art. 40	Art. 50, II	--	--	--	--	--
	Manter um código de conduta organizacional que inclua privacidade e proteção de dados	Art. 40	Art. 50, II	--	--	--	--	--
	Manter políticas / procedimentos para coleta e uso de dados pessoais e dados sensíveis	Art. 9, 10	Art. 11	--	--	Art. 2, §1, III; Art. 3, III	8.1.3	7.2.2, 7.2.4
	Manter políticas / procedimentos para coleta e uso de dados pessoais de crianças e menores	Art. 8, 12	Art. 14	1798.120 (c) 1798.120 (d)	--	--	8.1.3	7.2.2, 7.2.3,7.3.1,7.3.3,7.3.9

4. Incorporar privacidade e proteção de dados nas operações	Manter políticas / procedimentos para manter a qualidade dos dados	Art. 5	Art. 6	--	1,2,3, 4, 5, 6, 7,8,9,10, 11	--	6.2.1,7.2.2, 8.2.2,8.3.1,8.3.2,8.3.3,9.2.1 ,9.2.2,9.4.2,11.2.7,11.2.9,1 2.3.1,12.4.1,12.4.2,13.2.1,1 3.2.4,14.1.2,14.3.1,16.1.1,1 8.1.1,18.1.3	6.3.2.1,6.4.2.2,6.5.2.1,6.5.2.2,6.5.3.1,6.5. 3.2,6.5.3.3,6.6.2.1,6.6.2.2,6.6.4.2,6.8.2.7, 6.8.2.9,6.9.3.1,6.9.4.1,6.9.4.2,6.10.2.1,6.1 0.2.4,6.11.1.2,6.11.3.1,6.12.1.2,6.13.1.1,6 .15.1.1,6.15.1.3,7.2.1,7.2.2,7.2.6,7.2.8,7.3 .6,7.4.1,7.4.3,7.4.4,7.4.5,7.4.6,7.4.8,7.4.9, 8.2.2,8.4.1,8.4.3
	Manter políticas / procedimentos para a identificação de dados pessoais	Art. 30	Art. 37	1.798.130	--	--	--	--
	Manter políticas / procedimentos para revisar o tratamento total ou parcialmente por meios automatizados	Art. 12, 22	Art. 20	--	1,2,3, 7,8,10	--	8, 9.2, 9.4, 12, 13	--
	Manter políticas / procedimentos para usos secundários de dados pessoais	Art. 6, 13, 14	--	--	--	--	--	--
	Manter políticas / procedimentos para obter consentimento válido	Art. 6, 7, 8	Art. 8	1798.125 (b)(3), 1798.120 (d)	--	--	--	--
	Manter políticas / procedimentos para destruição segura de dados pessoais	Art. 5	Art. 6	--	--	--	--	--
	Integrar a privacidade e proteção de dados ao uso de cookies e mecanismos de rastreamento	--	--	--	--	--	--	--
	Integrar privacidade e proteção de dados em práticas de retenção de registros	Art. 5	Art. 16	--	1,2,3,4,5,6 7,8,9,10	--	8.2.2,8.3.1,8.3.2,8.3.3,9.2.1 ,9.2.2,9.4.2,11,12.3.1,12.4. 1,12.4.2,13.2.1,13.2.4,14.1. 2,14.3.1,16.1.1,18.1.1,18.1. 3	6.3.2.1,6.4.2.2,6.5.2.1,6.5.2.2,6.5.3.1,6.5. 3.2,6.5.3.3,6.6.2.1,6.6.2.2,6.6.4.2,6.8.2.7, 6.8.2.9,6.9.3.1,6.9.4.1,6.9.4.2,6.10.2.1,6.1 0.2.4,6.11.1.2,6.11.3.1,6.12.1.2,6.13.1.1,6 .15.1.1,6.15.1.3,7.2.1,7.2.2,7.2.6,7.2.8,7.3 .6,7.4.1,7.4.3,7.4.4,7.4.5,7.4.6,7.4.8,7.4.9, 8.2.2,8.4.1,8.4.3
	Integrar privacidade e proteção de dados em práticas de marketing direto	Art. 21, recital 43	--	--	1,2,3, 7,8,10	--	8.1.3, 9.2,9.4,12, 13	7.3.2,7.3.5
	Integrar a privacidade e proteção de dados nas práticas de marketing por email	Art. 21	--	--	--	--	--	--
	Integrar a privacidade e proteção de dados às práticas de telemarketing	Art. 21	--	--	--	--	--	--
	Integrar a privacidade e proteção de dados às práticas de marketing digital (por exemplo, celular, mídia social, publicidade comportamental)	Art. 21, recital 43	--	--	--	--	--	--
	Integrar a privacidade e proteção de dados nas práticas de contratação	--	--	--	--	--	7.1,15	--
	Integrar a privacidade de dados ao uso de práticas de mídia social da organização	Art. 8	--	--	--	--	8.1.3	7.2.2,7.2.3
	Integrara privacidade e proteção de dados nas políticas / procedimentos Bring Your Own Device (BYOD), se houver	--	--	--	9	--	6.2,8.1.2,8.1.3,11.2	--
	Integrar a privacidade e proteção de dados nas práticas de saúde e segurança	--	--	--	--	--	--	--
	Integrar a privacidade e proteção dos dados nas interações com os conselhos de empresa	--	--	--	--	--	--	--
	Integrar a privacidade e proteção de dados em práticas para monitorar funcionários	--	--	--	--	--	7.2,7.3,12.4	--
	Integrar a privacidade e proteção de dados ao uso de vigilância de CFTV / vídeo	--	--	--	--	--	8.1.3	--
	Integrar a privacidade e proteção de dados ao uso de dispositivos de localização geográfica (rastreamento e / ou localização)	--	--	--	--	--	8.1.3	--
	Integrar a privacidade dos dados no acesso delegado às contas de email da empresa dos funcionários (por exemplo, férias, LOA, rescisão)	--	--	--	--	--	8.1.3	--
	Integrar a privacidade e proteção de dados às práticas de descoberta eletrônica	--	--	--	--	--	8.1.3, 9.2,9.4.4,12.7	--
	Integrar a privacidade e proteção dos dados na condução de investigações internas	--	--	--	--	--	12.7	--
	Integrar a privacidade e proteção de dados em práticas para divulgação e para fins de aplicação da lei	--	Art. 50, §3º	--	--	--		--
	Integrar a privacidade e proteção de dados nas práticas de pesquisa	Art. 21, 89	Art. 13	1798.140 (s) - correlata	1,2,3, 7,8,10	--	8.1.3, 9.2, 9.4, 12.4, 12.7,13	7.3.2,7.3.5
5. Manter programa de treinamento e conscientização	Conduzir treinamento em privacidade e proteção de dados	Art. 39	Art. 41,50,	--	--	Art. 3, VI, a	7.2.2	6.3.1.1,6.4.2.2
	Conduzir treinamento de privacidade e proteção de dados para atividades específicas	Art. 43	Art. 41, III	1798.135 (a)(3), 1798.130 (a)(6)	--	Art. 3, VI, a	7.2.2	--
	Conduzir treinamentos periódicos de reciclagem	--	--	--	--	Art. 3, VI, a	7.2.2	--
	Incorporar a privacidade e proteção dos dados ao treinamento operacional, como RH, segurança, call center	Art. 39	Art. 41, III	--	--	Art. 3, VI, a	7.2.2	--
	Oferecer treinamento / conscientização em resposta a questões / tópicos que vierem a surgir oportunamente	Art. 39	Art. 41, III	--	--	Art. 3, VI, a	7.2.2	--
	Desenvolver e publicar boletim de privacidade e proteção de dados ou incorporar a privacidade e proteção de dados às comunicações corporativas existentes	--	--	--	--	Art. 4	--	--
	Fornecer um repositório de informações de privacidade e proteção de dados, por exemplo, uma intranet interna de privacidade e e proteção de dados	--	--	--	--	Art. 4	--	--
	Manter e disponibilizar material de conscientização de privacidade e proteção de dados (por exemplo, pôsteres e vídeos)	Art. 39	Art. 41, III	--	--	Art. 4	7.2.2	--
	Realizar eventos de conscientização de privacidade e proteção de dados (por exemplo, um dia / semana anual de privacidade de dados)	Art. 39	Art. 41, III	--	--	Art. 4	7.2.2	--
	Avaliar a participação em atividades de treinamento em privacidade e proteção de dados (por exemplo, número de participantes, pontuação)	Art. 39	Art. 41, III	--	--	Art. 3, VI, a	--	--
	Adotar e aplicar requisito para conclusão de treinamento em privacidade e proteção de dados	--	--	--	--	--	--	--

	Fornecer educação e treinamento contínuos para o Privacy Office e / ou DPOs (por exemplo, conferências, seminários on-line, palestrantes convidados)	Art. 39	Art. 41, III	--	--	--	--	--
	Manter a certificação dos responsáveis pela privacidade e proteção dos dados, incluindo a educação profissional continuada	--	--	--	--	--	--	--
6. Gerenciar riscos de segurança da informação	Integrar o risco de privacidade e proteção de dados nas avaliações de risco de segurança	Art. 32	Art. 50	--	1,2,3, 4,5,6,7,8,10,11,12	--	5.1, 6.1.2,6.2,8 ,10,12.3.1, 14.1.2,15.1.2,18.1.1,18.2.1, 18.2.3	5.2.1,5.2.3,5.2.4,5.4.1.2,5.4.1.3, 6.9.3.1,6.11.1.2,6.12.1.2,6.15.1.1,6.15.2.1 ,6.15.2.3,7.2.1,7.4.5,8.2.2
	Integrar privacidade e proteção de dados em uma política de segurança da informação	Art. 5,32	Art. 6, 46, 49	--	1,2,3,4,5,6, 7,8,9,10, 11, 12	Art. 2	5.1, 6.1.2,6.2,6.2.1,7.2.2, 8.2.2,8.3.1,8.3.2,8.3.3,9.2.1 ,9.2.2,9.4.2,10,11.2.7,11.2. 9,12.3.1,12.4.1,12.4.2,13.2. 1,13.2.4,14.1.2,14.3.1, 15.1.2,16.1.1,18.1.1,18.1.3, 18.2.3	5.2.1,5.2.3,5.2.4,5.4.1.2,5.4.1.3,6.3.2.1,6. 4.2.2,6.5.2.1,6.5.2.2,6.5.3.1,6.5.3.2,6.5.3. 3,6.6.2.1,6.6.2.2,6.6.4.2,6.8.2.7,6.8.2.9,6. 9.3.1,6.9.4.1,6.9.4.2,6.10.2.1,6.10.2.4,6.1 1.1.2,6.11.3.1,6.12.1.2,6.13.1.1,6.15.1.1, 6.15.1.3, 6.15.2.1, 6.15.2.3, 7.2.1,7.2.2,7.2.6,7.2.8,7.3.6,7.4.1,7.4.3,7. 4.4,7.4.5,7.4.6,7.4.8,7.4.9,8.2.2,8.4.1,8.4. 3
	Manter medidas técnicas de segurança (por exemplo, detecção de intrusões, firewalls, monitoramento)	Art. 32	Art. 46	--	1,2,3,4,5,6, 7,8,9,10	Art. 3, II e §2	6.1.2, 6.2,8.3, 9, 11.2,12.2,12.4,12.5,12.6, 13, 14	5.2.1,5.2.3,5.2.4,5.4.1.2,5.4.1.3, 6.9.3.1,6.11.1.2,6.12.1.2,6.15.1.1,6.15.2.1 ,6.15.2.3,7.2.1,7.4.5,8.2.2
	Manter medidas para criptografar dados pessoais	Art. 32	--	--	--	Art. 3, II e §2	10, 18.1.5	5.2.1,5.2.3,5.2.4,5.4.1.2,5.4.1.3, 6.9.3.1,6.11.1.2,6.12.1.2,6.15.1.1,6.15.2.1 ,6.15.2.3,7.2.1,7.4.5,8.2.2
	Manter um uso aceitável da política de recursos de informação	--	--	--	--	--	8.1	
	Manter procedimentos para restringir o acesso a dados pessoais (por exemplo, acesso baseado em função, segregação de funções)	Art. 32	--	--	--	Art. 3, II e §2	8.1.3, 9,12.4	5.2.1,5.2.3,5.2.4,5.4.1.2,5.4.1.3, 6.9.3.1,6.11.1.2,6.12.1.2,6.15.1.1,6.15.2.1 ,6.15.2.3,7.2.1,7.4.5,8.2.2
	Integrar a privacidade e proteção de dados a uma política de segurança corporativa (proteção de instalações físicas e ativos físicos)	--	--	--	9	Art. 3, II e §2	11	--
	Manter medidas de segurança de recursos humanos (por exemplo, pré-triagem, avaliações de desempenho)	--	Art. 47	--	--	--	7.1,7.2.3,7.3	--
	Manter planos de backup e continuidade de negócios	--	--	--	--	Art. 3, II, V, a, e §2, Art. 8, Art. 16, IV, Art. 19	12.3, 17	6.9.3
	Manter uma estratégia de prevenção de perda de dados	--	--	--	--	--	17.2	--
	Conduzir testes regulares quanto ao desempenho de segurança de dados	Art. 32	--	--	--	Art. 3, II e §2, Art. 21	18.2.1	5.2.1,5.2.3,5.2.4,5.4.1.2,5.4.1.3, 6.9.3.1,6.11.1.2,6.12.1.2,6.15.1.1,6.15.2.1 ,6.15.2.3,7.2.1,7.4.5,8.2.2
	Manter uma certificação de segurança (por exemplo, ISO)	Art. 43	--	--	--	Art. 24, II	--	--
7. Gerenciamento de Riscos de Terceiros	Manter política de privacidade e proteção de dados para terceiros (por exemplo, clientes, fornecedores, processadores, afiliados)	Art. 28, 32	Art. 39	1798.130 (6) 1798.140 (w) (b)	--	--	6.1.4, 15	5.2.1,6.10.2.4,6.12.1.2,6.15.1.1,7.2.6,8.2. 4,8.2.5,8.56.,8.5.7,8.5.85.2.3,5.2.4,5.4.1.2 ,5.4.1.3, 6.9.3.1,6.11.1.2,6.12.1.2,6.15.1.1,6.15.2.1 ,6.15.2.3,7.2.1,7.4.5,8.2.2
	Manter procedimentos para executar contratos ou acordos com todos os processadores	Art. 28, 32	Art. 39	1798.105 (c) - obrigação correlata com este item	4,5,6	Art. 11 à 18	13.2, 14.1, 15, 18.1.2, 18.2.2	5.2.1,6.10.2.4,6.12.1.2,6.15.1.1,7.2.6,8.2. 4,8.2.5,8.56.,8.5.7,8.5.8
	Realizar a devida diligência em torno da postura de privacidade e proteçãode dados, segurança de dados de fornecedores / operadores em potencial	Art. 28	Art. 39	1798.130 (6)- correlata 1798.135 (3) - correlata 1798.140 (w) (b) - correlata 1798.145 (k) - correlata	--	Art. 21	13.2.4,15.1.2, 18	5.2.1,6.10.2.4,6.12.1.2,6.15.1.1,7.2.6,8.2. 4,8.2.5,8.56.,8.5.7,8.5.8
	Realizar due diligence em fontes de dados de terceiros	--	--	--	--	Art. 21	--	--
	Manter um processo de avaliação de risco de privacidade e proteção de dados do fornecedor	--	Art. 39	1798.140 (w) (b) 1798.145 (k)	--	Art. 6	15	--
	Manter uma política que rege o uso de provedores de nuvem	--	--	--	--	Art. 11 à 18	9.1,13, 15, 18	--
	Manter procedimentos para lidar com casos de não conformidade com contratos e acordos	--	--	1798.140 (w) (b)	--	--	--	--
	Conduzir diligência em torno da postura de privacidade e proteção de dados, segurança de dados de fornecedores / processadores	Art. 28	Art. 39	1798.140 (w) (b)	--	Art. 21	--	--
	Analisar os contratos de longo prazo para verificar riscos de privacidade de dados novos ou em evolução	--	--	--	--	--	13.2.4, 15, 18	--
8. Atualizar os avisos	Manter um aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização	Art. 8, 13, 14	Art. 6, 7, 9, 14	1798.100 (b) 1798.105 (b) 1798.115 (a)-(d) 1798.120 (b) 1798.125 (b)(2) 1798.135 (a)(2) 1798.185 (6)	--	Art. 4 e 5	8	7.2.2,7.2.3,7.3.2,7.3.3,7.3.4,7.3.5,7.3.6,7. 3.10,7.4.7,
	Fornecer aviso de privacidade e proteção de dados em todos os pontos em que os dados pessoais são coletados	Art. 13, 14, 21	Art. 9, 14	1798.100(b)	1,2,3, 7,8, 9,10	Art. 4 e 5	8, 9.2, 9.3, 9.4, 11.1, 12, 13, 18.1.1	7.3.2,7.3.3,7.3.4,7.3.5,7.3.6,7.3.10,7.4.7
	Fornecer aviso nas comunicações de marketing (por exemplo, e-mails, folhetos, ofertas)	Art. 13,14	Art. 6	1798.100 (b) 1798.105 (b) 1798.115 (a)-(d) 1798.120 (b) 1798.125 (b)(2) 1798.135 (a)(2) 1798.185 (6)	--	--	--	--
	Fornecer aviso em contratos e termos	Art. 13,14	Art. 6	1798.100 (b) 1798.105 (b) 1798.115 (a)-(d) 1798.120 (b) 1798.125 (b)(2) 1798.135 (a)(2) 1798.185 (6)	--	--	15	--
	Manter scripts para uso dos funcionários para explicar ou fornecer o aviso de privacidade e proteção de dados	Art. 13,14	Art. 6	--	--	--	--	--

	Manter um selo de privacidade e proteção de dados ou marca de confiança para aumentar a confiança do cliente	--	--	--	--	--	--	--
9. Responder a solicitações e reclamações dos Titulares de Dados	Manter procedimentos para tratar de reclamações	Art. 24, §2º	Art. 50	1798130 1798.185 (a) (7)	--	--	--	--
	Manter procedimentos para responder a solicitações de acesso a dados pessoais	Art. 15	Art. 6, 18, 19	1798.100(a) 1798.130 1798.185 (a) (7)	1,2,3, 7,8,10	--	9.1.2,9.2, 12.4, 13.2	7.3.2,7.3.9,7.5.1,7.5.2,8.3.1
	Manter procedimentos para responder a solicitações e / ou fornecer um mecanismo para os indivíduos atualizarem ou corrigirem seus dados pessoais	Art. 16, 19	Art. 18	1798130 1798.185 (a) (7) - não tem direito a retificação ou atualização. Apenas solicitar informações	1,2,3, 7,8,10	--	9.1.2,9.2, 12.4, 13.2	7.3.6,7.3.7
	Manter procedimentos para responder a pedidos de exclusão, restrição ou oposição ao processamento	Art. 7, 18, 21	Art. 8 (5), 18, 20	1798.105 (a); 1798.115 (d) 1798.120 (a) 1798.130, 1798.135 (a)(1)-(6) e (c) 1798.130 1798.185 (a) (7) - não há direito de restrição	1,2,3, 7,8,10	--	9.1.2,9.2, 12.4, 13.2	7.2.2,7.3.2,7.2.4, 7.3.3,7.3.4, 7.3.5,8.2.3
	Manter procedimentos para responder a pedidos de informações	Art. 12	Art. 18	1798.110 (a) 1798.110 (b) 1798.115 (a) 1798.115 (b) 1798.115 (c) 1798.130 1798.185 (a) (7)	--	--	--	--
	Manter procedimentos para responder a solicitações de portabilidade de dados	Recital 45, 47, 55 Art. 20	Art. 18	1798.100 (d) second, 1798.130 1798.185 (a) (7)	--	--	13.2	7.3.8
	Manter procedimentos para responder a pedidos a serem esquecidos ou para apagar dados	Recital 45, 47, 53, 54 Art. 17, 19	Art. 18	1798.105 (a) 1798.130 1798.185 (a) (7)	1,2,3, 7,8,10	--	9.1.2,9.2, 12.4, 13.2	7.2.2,7.3.6,7.3.7
	Manter perguntas freqüentes (FAQ) para responder a perguntas de indivíduos	Art. 13,14	Art. 6	--	--	--	--	--
	Investigar as causas raizes das reclamações de proteção de dados	--	--	--	--	--	--	--
	Monitorar e reportar métricas para reclamações de privacidade e proteção de dados (por exemplo, quantidade, causa raiz)	--	--	--	--	Art. 3, III	--	--
10. Monitorar Novas Práticas Operacionais	Manter procedimento de verificação de identidade dos titulares	--	--	1798.100 (c) 1798.105 (c) 1798.110 (b) 1798.115 (b) 1798.130 (a) (2) 1798.130 (a) (3) (7) 1798.140 (y)	--	--	--	--
	Integrar o Privacy by Design no desenvolvimento de sistemas e produtos da organização	Art. 25	Art. 46	--	12	Art. 3, §3	5,6, 10,14.2	5.2.1, 6.11.2.1,6.11.2.5,7.4.2,
	Manter diretrizes e modelos do RIPD/ DPIA/ PIA/ LIA	Recital 70a, Art. 35	Art. 5, XVII, 38	--	--	--	18.1.1	5.2.2,7.2.5
	Conduzir RIPD/ DPIA/ PIA para novos programas, sistemas, processos que envolva tratamento de dados pessoais	Recital 66a, 70-72, 74 Art. 5, 6, 25, 35	Art. 38	--	4,5,6, 11, 12	--	5,6,14.2, 14.3,16.1.1,18.1.1,18.1.3	5.2.2, 6.3.2.1,6.4.2.2,6.5.2.1,6.5.2.2,6.5.3.1,6.5.3.2,6.5.3.3,6.6.2.1,6.6.2.2,6.6.4.2,6.8.2.7, 6.8.2.9,6.9.3.1,6.9.4.1,6.9.4.2,6.10.2.1,6.10.2.4,6.11.1.2, 6.11.2.1, 6.11.2.5, 6.11.3.1,6.12.1.2,6.13.1.1,6.15.1.1,6.15.1.3,7.2.1,7.2.2, 7.2.5, 7.2.6,7.2.8,7.3.6,7.4.1, 7.4.2, 7.4.3,7.4.4,7.4.5,7.4.6,7.4.8,7.4.9,8.2.2,8.4.1,8.4.3
	Conduzir RIPD/ DPIA/ PIA para alterações nos programas, sistemas ou processos existentes que envolva tratamento de dados pessoais	Art. 5, 6, 25, 35	--	--	4,5,6	--	9.4.5, 12.1.1,12.1.2,12.1.4, 14.2.2,14.2.8,14.3, 18.1.1	5.2.2, 6.3.2.1,6.4.2.2,6.5.2.1,6.5.2.2,6.5.3.1,6.5.3.2,6.5.3.3,6.6.2.1,6.6.2.2,6.6.4.2,6.8.2.7, 6.8.2.9,6.9.3.1,6.9.4.1,6.9.4.2,6.10.2.1,6.10.2.4,6.11.1.2, 6.11.2.1, 6.11.2.5, 6.11.3.1,6.12.1.2,6.13.1.1,6.15.1.1,6.15.1.3,7.2.1,7.2.2, 7.2.5, 7.2.6,7.2.8,7.3.6,7.4.1, 7.4.2, 7.4.3,7.4.4,7.4.5,7.4.6,7.4.8,7.4.9,8.2.2,8.4.1,8.4.3
	Envolver as partes interessadas externas como parte do processo da RIPD/ DPIA/ PIA	Art. 35	--	--	--	--	4.2, 6.1.4	5.2.2,7.2.5
	Rastrear e solucionar problemas de proteção de dados identificados durante RIPD/ DPIA/ PIA	Art. 35	--	--	4,5,6	--	14.2.2, 14.2.3,14.3,18.1.4	5.2.2,7.2.5
	Relatar a análise e os resultados do RIPD/ DPIA/ PIA aos reguladores (quando necessário) e partes interessadas externas (se apropriado)	Art. 36	--	--	--	--	4.2, 18.1.4, 6.1.4	5.2.2,7.2.5,
11. Manter o programa de gerenciamento de violação de privacidade e proteção de dados	Manter um plano de resposta a incidentes / violações da privacidade de dados	Art. 33, 34	Art. 48, 5	1798.150 - correlata; 1798.150 (b)	--	Art. 6	16	6.13.1.1,6.13.1.5,
	Manter um protocolo de notificação de violação (para as pessoas afetadas) e relatórios (para reguladores, agências de crédito, órgãos policiais)	Art. 12, 33, 34	Art. 48	--	--	--	4.2, 6.1.3,16.1.1, 16.1.5, 18.1.1	6.13.1.1,6.13.1.5, 7.3.1,7.3.3,7.3.9,
	Manter o registro quanto o rastreamento de incidentes / violações de privacidade e proteção de dados	Art. 33	--	--	--	Art. 8, §1, III	16.1.2	6.13.1.1,6.13.1.5,
	Monitorar e reportar as métricas de incidentes / violações de privacidade e proteção de dados (por exemplo, natureza da violação, risco, causa raiz)	--	--	--	--	Art. 8	16.1.3	--
	Realizar testes periódicos do plano de violação / incidente de privacidade e proteção de dados (exemplo pentest)	--	--	1798.150 - correlata; 1798.150 (b)	--	Art. 21, §2	17.1.3	--
	Envolver uma equipe de investigação forense	--	--	--	--	--	--	--

	Obter cobertura de seguro de violação de privacidade e proteção de dados	--	--	--	--	--	17	--
12. Monitoramento de Tratamento de Dados	Conduzir auto-avaliações de gerenciamento de privacidade e proteção de dados	Art. 24,25, 39	Art. 50	--	--	--	5.1.2,17.1.3,18	5.2.1,6.2.1.1,6.3.1.1, 6.4.2.2, 6.15.1.3,7.2.8,
	Conduzir auditorias internas do programa de privacidade e proteção de dados (ou seja, auditoria operacional do Privacy Office)	Art. 25	Art. 50	--	--	Art. 3, VI, a	9.2, 17.1.3	--
	Conduzir walk-throughs (treinamentos/orientações) periódico	Art. 39	Art. 41,III	--	--	--	7.2.2	--
	Conduzir avaliações com base em eventos externos, como reclamações / violações, entre outros	Art. 12, 34	Art. 18, 46,48	--	--	--	16.1.2	--
	Envolver a auditoria externas para avaliações independentes	Art. 25	Art. 50	--	--	--	18.2.1	--
	Monitorar e reportar as métricas de privacidade e proteção de dados	--	--	--	--	Art. 21	--	--
	Manter a documentação como evidência a fim de demonstrar conformidade e / ou prestação de conta	Art. 5, 24	Art. 6, 50	--	12	Art. 2, Art. 10, Art. 12, §2, Art. 16, §3,Art. 17, PU, I, Art. 23	5,12.1.1,13.2.2,17.1.2, 18.2	5.2.1, 6.2.1.1, 6.3.2.1,6.4.2.2,6.5.2.1,6.5.2.2,6.5.3.1,6.5.3.2,6.5.3.3,6.6.2.1,6.6.2.2,6.6.4.2,6.8.2.7,6.8.2.9,6.9.3.1,6.9.4.1,6.9.4.2,6.10.2.1,6.10.2.4,6.11.1.2,6.11.3.1,6.12.1.2,6.13.1.1,6.15.1.1,6.15.1.3,7.2.1,7.2.2,7.2.6,7.2.8,7.3.6,7.4.1,7.4.3,7.4.4,7.4.5,7.4.6,7.4.8,7.4.9, 8.2.2,8.4.1,8.4.3
	Manter certificações, acreditações ou selos de proteção de dados para demonstrar conformidade com os reguladores	Art. 42	--	--	--	Art. 12, II, d; Art. 17, V, b; Art. 24, II	--	--
13. Rastrear critérios externos	Identificar e/ou monitorar as obrigatoriedades/ requerimento e as melhorias contínuas de conformidade com a privacidade e e proteção de dados, por exemplo, lei, jurisprudência, códigos etc.	Art. 39	Art. 50	--	12	--	5.1, 13.2.4, 18.1.1	6.3.1.1,6.4.2.2
	Atender/ participar de eventos, conferências de privacidade, associações do setor, entre outros	--	--	--	--	--	--	--
	Registro / relatório sobre o rastreamento de novas leis, regulamentos, emendas, boas práticas, entre outros	--	--	--	--	--	18.1.1	--
	Monitorar e buscar pareceres jurídicos sobre projetos de leis recentes	--	--	--	--	--	--	--
	Documentar as decisões em torno de novos requisitos/exigências, incluindo sua implementação ou qualquer justificativa por trás de decisões para não implementar mudanças/ recomendações	Art. 25	--	--	--	--	--	--
	Identificar e gerenciar conflitos legais	--	--	--	--	--	--	--

O ponto de partida desse material foi "Nymity-GDPR-Readiness-Questions", o qual foi adequado para fins deste comparativo.

Material elaborado pelo LGPD Acadêmico - Creative Common - Versão 1 - 17.02.2020
Coordenado por Remilina Yun (Remi)
Colaboradores: Angela Maria Rosso, Fernanda Maia, Gustavo Godinho, Rachel Gonzaga, Remilina Yun (Remi)