A LEI GERAL DE PROTEÇÃO DE DADOS: UM ESTUDO DESCRITIVO E EXPLORATÓRIO DA SUA APLICAÇÃO NO BRASIL E NO CENÁRIO INTERNACIONAL

*Ricardo Alexandre Costa**

*Carlos Renato Cunha***

RESUMO

Este artigo apresenta um estudo descritivo e exploratório sobre a Lei Geral de Proteção de Dados (LGPD) no Brasil e no contexto internacional. O objetivo é analisar a legislação, suas implicações e compará-la com outros marcos regulatórios. O estudo é conduzido por meio dos seguintes aspectos: a) Inovações Tecnológicas e Proteção Jurídica de Dados Pessoais no Ciberespaço: Uma Necessidade Mundial Explora-se a crescente importância das inovações tecnológicas e a necessidade de proteção jurídica dos dados pessoais no ambiente online em escala global. Serão discutidos os desafios e riscos relacionados à privacidade e segurança dos indivíduos nesse contexto. b) Antecessores Legais da LGPD no Brasil: Resumo Conciso Apresenta-se um resumo conciso das leis e regulamentos que antecederam

* Mestre pelo Programa de Mestrado Profissional em Direito, Sociedade e Tecnologias, da Escola de Direito das Faculdades Londrina/PR. Titular do Cartório de Protestos da Comarca de Foz do Iguaçú PR. Paraná (Brasil). E-mail: tabeliaoricardocosta@gmail.com.

** Professor vinculado ao Programa de Mestrado Profissional em Direito, Sociedade e Tecnologias da Escola de Direito das Faculdades Londrina. Doutor e Mestre em Direito do Estado pela UFPR. Especialista em Direito Tributário pelo IBET. Procurador do Município de Londrina. Advogado. E-mail: carlosrenato80@gmail.com

a LGPD no Brasil. Serão destacadas as principais características desses marcos regulatórios prévios, mostrando a evolução até a promulgação da LGPD. C) Direito Comparado: LGPD e RGPD Realiza-se uma comparação entre a LGPD brasileira e o Regulamento Geral de Proteção de Dados (RGPD) europeu. São exploradas as semelhanças e diferenças entre essas legislações, analisando os princípios e requisitos fundamentais para a proteção de dados pessoais em ambos os contextos. d) Proteção Jurídica de Dados Pessoais em Perspectiva: Estados Unidos e Japão Examina-se a perspectiva da proteção jurídica de dados pessoais nos Estados Unidos e Japão. Serão abordados os marcos legais e regulatórios desses países, bem como suas abordagens específicas e desafios relacionados à privacidade e proteção de dados. Este estudo descritivo e exploratório visa fornecer uma análise abrangente da LGPD, situando-a tanto no contexto nacional quanto internacional. Ao comparar com outros marcos regulatórios e analisar diferentes perspectivas, busca-se compreender melhor os impactos e desafios da proteção de dados pessoais.
Palavras chave: Lei Geral de Proteção de Dados; Inovação Tecnológica; Internacional.

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo, ela tem sido de grande relevância no Brasil e no cenário internacional, visto que se tornou fundamental estabelecer diretrizes para proteger a privacidade dos indivíduos e garantir o uso adequado de informações.

No Cenário Brasileiro a LGPD entrou em vigor em 2020. Ela estabelece diretrizes claras sobre como empresas e organizações devem coletar, armazenar, processar e compartilhar dados pessoais, com o objetivo de proteger a privacidade dos indivíduos e dar-lhes maior controle sobre suas informações. A lei também prevê a criação da Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar e garantir o cumprimento das disposições legais.

No cenário internacional, dois países que se destacam na proteção de dados são o Japão e os Estados Unidos. O Japão possui a Lei de Proteção de

Informação Pessoal (APPI), que entrou em vigor em 2005 e foi revisada em 2022 para se adequar aos padrões internacionais. Já os Estados Unidos não possuem uma lei federal de proteção de dados abrangente, mas contam com várias leis setoriais e estaduais, como o California Consumer Privacy Act (CCPA) e o General Data Protection Regulation (GDPR), na União Europeia.

Assim, com base no presente estudo se buscará analisar as semelhanças e diferenças da aplicação dessa Lei, bem como compreender a dificuldade enfrentada em cada País. Além disso, também será possível avaliar os impactos da LGPD na proteção da privacidade dos indivíduos, na economia e nas relações comerciais.

2 AS INOVAÇÕES TECNOLÓGICAS E A PROTEÇÃO JURÍDICA DOS DADOS PESSOAIS NO CIBERESPAÇO: UMA NECESSIDADE MUNDIAL

Atualmente vive-se em uma sociedade em que a informação é o elemento base para o desenvolvimento econômico e pode ser transmitida em quantidade e velocidade nunca vista. Harari (2017), em seu best-seller *Sapiens*, apresenta uma situação bastante intrigante: o mundo ainda seria familiar para um camponês que adormecesse, no ano 1000, por quinhentos anos, acordando de seu sono com a chegada dos marinheiros de Colombo no ano 1500, porém seria totalmente estranho a um marinheiro em situação similar ao ser despertado ao toque de um iPhone do século XXI.

Da mesma forma, Castells (2011, p. 53-54) apresenta a diferenciação entre os modos de desenvolvimento anteriores à revolução causada pela internet (agrária e industrial) e destacada a centralidade atual da informação, confirmando que as TICs foram determinantes para a evolução do capitalismo e a sua atual dimensão.

> Cada modo de desenvolvimento é definido pelo elemento fundamental à promoção da produtividade no processo produtivo. Assim, no modo agrário de desenvolvimento, a fonte do incremento de excedente resulta dos aumentos quantitativos da mão-de-obra e dos recursos naturais (em parti-

> cular) no processo produtivo, bem como da dotação natural desses recursos. No modo de desenvolvimento industrial, a principal fonte de produtividade reside na introdução de novas fontes de energia e na capacidade de descentralização do uso de energia ao longo dos processos produtivo e de circulação. No novo modo informacional de desenvolvimento, a fonte de produtividade acha-se na tecnologia de geração de conhecimentos, de processamento da informação e de comunicação de símbolos. [...], o que é específico ao modo informacional de desenvolvimento é a ação de conhecimentos sobre os próprios conhecimentos como principal fonte de produtividade. O processamento da informação é focalizado na melhoria da tecnologia do processamento da informação como fonte de produtividade, em um círculo virtuoso de interação entre as fontes de conhecimentos tecnológicos e a aplicação da tecnologia para melhorar a geração de conhecimentos e o processamento da informação.

Considerando as características peculiares (meio de comunicação diferente em muitos aspectos da interação tradicional, por exemplo) e o alcance (ilimitado e globalizado) da Rede, observou-se, ainda na década de 1990, a necessidade da criação de um direito do ciberespaço, separado do direito convencional, que garantisse o cumprimento dos direitos fundamentais, principalmente o direito fundamental à proteção de dados pessoais.

Ao escrever sobre a revolução digital e sua influência no judiciário, Araújo e Gomes (2022) afiançam que a aceleração tecnológica impacta o comportamento das pessoas, bem como os setores mais tradicionais da economia. Os autores apresentam a "quarta revolução industrial" [1], que trata da "[...] revolução tecnológica que alterará fundamentalmente a maneira como vivemos, trabalhamos e nos relacionamos uns com os outros" (ARAÚJO; GOMES, 2022, p. 107 [tradução nossa] [2]). Segundo os autores, essa transformação digital:

> [...] tem sido recorrentemente mencionada e trazida à tona, dada a sua relevância não somente de impacto em nossas vidas como também pela sua escala, abrangência e complexidade. Iniciou-se no bojo da terceira revolução industrial, então chamada de Revolução Digital, que mudou radicalmente a sociedade, as formas de comunicação e o estado do mundo globalizado (ARAÚJO; GOMES, 2022, p. 107).

1 Termo apresentado por Klaus Schwab no Fórum Econômico Mundial de 2016.

2 "technological revolution that will fundamentally alter the way we live, work, and relate to one another"

O sociólogo Castells (2011, p. 119) denomina como "Terceira Revolução Industrial" e apresenta seus conceitos:

> Uma nova economia surgiu em escala global no último quartel do século XX. Chamo-a de informacional, global e em rede para identificar suas características fundamentais e diferenciadas e enfatizar sua interligação. É informacional porque a produtividade e a competividade de unidades ou agentes nessa economia (sejam empresas, regiões ou nações) dependem basicamente de sua capacidade de gerar, processar e aplicar de forma eficiente a informação baseada em conhecimentos.
> É global porque as principais atividades produtivas, o consumo e a circulação, assim como seus componentes (capital, trabalho, matéria--prima, administração, informação, tecnologia e mercados) estão organizados em escala global, diretamente ou mediante uma rede de conexões entre agentes econômicos. É rede porque, nas novas condições históricas, a produtividade é gerada, e a concorrência é feita em uma rede global de interação o entre redes empresariais.

Neste contexto, em que a inovação tecnológica, indiscutivelmente, dinamiza a comunicação, por um lado, e potencializa a captação, o armazenamento e envio de dados e informações, abusos podem ser cometidos, por outro lado. Sobre as inovações tecnológicas e a necessidade de o Direito intervir pela proteção jurídica dos dados pessoais no ciberespaço, Araújo e Gomes (2022, p. 11) afirmam que

> [...] os novos tempos chegam e o verdadeiro desafio de quem atua profissionalmente com o Direito é o de identificar, nas inovações tecnológicas, as oportunidades de progresso para a humanidade. [...] a fim de promover modelos inovadores de aplicação do Direito em linha com a eficiência e o atendimento aos anseios sociais.

No mesmo viés, Barroso (2022, p. 33) afiança que

> A internet trouxe a democratização do acesso à informação e ao espaço público, mas suprimiu, em ampla medida, a intermediação do jornalismo profissional, que fora a marca do último século. Com ela vieram, também, a invasão de privacidade, a difusão da mentira deliberada e de notícias falsas, condutas utilizadas como estratégia de chegada ao poder e de desmoralização das instituições democráticas.

Boff e Fortes (2014) já afiançavam, mesmo antes da LGPD, que a construção de um modelo normativo de governança do ciberespaço deveria, indispensavelmente, respeitar as premissas de construção da Web, sem que ocorram rupturas paradigmáticas com a arquitetura adotada com a sua constituição e com a constante adaptação que culminou na constituição da cibercultura e do ciberespaço.

Além disso, segundo Bortali (2020), atualmente, todo indivíduo já está acostumado a realizar cadastros *on-line* para acessar conteúdos digitais, incluindo os sítios eletrônicos de serviços governamentais, que exigem cadastro completo para acessar determinada informação. Iramina (2020, p. 92) ressalta, no mesmo sentido, que:

> Em uma sociedade cada vez mais informatizada, na qual o fluxo de dados se tornou um componente crucial para o comércio, as comunicações e as interações sociais, a proteção de dados pessoais passou a ser uma preocupação para grande parte dos países. Nesse contexto, muitos países têm adotado novas regras de proteção de dados ou modernizado as que já tinham, como Coreia do Sul, Chile, Tailândia, Índia, Indonésia e Brasil. Atualmente, já são mais de cem países com marcos regulatórios para proteção de dados pessoais em todo o mundo.

Assim, entende-se que a era da informação disponibiliza maravilhosas inovações tecnológicas à sociedade, porém, recentemente os impactos, positivos e negativos, destes avanços começam a ser mensurados. "Toda beleza e eficiência dos recursos tecnológicos e das possibilidades de interação travam uma batalha fervorosa com a privacidade, lembrando que esta já possui garantia constitucional [...]" (PINHEIRO, 2019). Micheletti e Borges (2021) concordam que a sociedade brasileira está passando por profundas e aceleradas transformações, impulsionadas pelas inovações tecnológicas.

Boff e Fortes (2014), ao fazer referência à privacidade e à proteção dos dados pessoais no ciberespaço, afirmam que a evolução tecnológica e a inclusão digital (democratização do acesso à internet) refletiram na exposição maciça de informação no ciberespaço, o que "[...] oferece novas e diferentes possibilidades de futuro, mas pode representar uma afronta aos direitos fundamentais da privacidade e da proteção aos dados pessoais".

Bortali (2020) informa que, ao longo da história, diversas criações legislativas foram promulgadas a fim de proteger dados, citando as leis: do

Estado Alemão de Hesse (1970), Lei de Dados da Suécia (1973), Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974), e Lei Federal de Proteção de Dados da Alemanha (1977). Porém, foi na União Europeia (UE) que o Brasil – e outros países, já que é a UE que apresenta a base legal mais completa sobre o tema, sendo um exponencial na legislação sobre proteção de dados – buscou tendências para a constitucionalização da proteção de dados, deixando manifesta a convergência de orientações entre as legislações adotadas.

A exemplo do ocorrido no cenário mundial, a Lei Geral de Proteção de Dados (LGPD) foi estabelecida no Brasil para prezar rigorosamente pela proteção à privacidade e dar proteção jurídica aos dados pessoais (BASTOS; BASI; CASSI, 2021). O surgimento de regulamentações para proteção de dados, no mundo e no Brasil, tem como motivação os avanços do modelo de negócios da economia digital (PINHEIRO, 2021), as inovações tecnológicas, o alargamento do uso da internet (RUSSO, 2019), fomentado pela pandemia do Covid-19 e pela necessidade de isolamento social (PINHEIRO, 2021).

Apresenta-se, *a priori*, um breve histórico, que demonstrará os antecessores legais da proteção jurídica aos dados pessoais no Brasil. Além disso, na tentativa de demonstrar a operacionalização da proteção de dados pessoais, faz-se, nesta seção, a comparação entre a lei brasileira e a lei europeia e, após, a apresentação de elementos da proteção de dados pessoais em outros países de relevância econômica e tecnológica, Estados Unidos e Japão.

3 ANTECESSORES LEGAIS DA LGPD NO BRASIL: BREVE RESUMO

De acordo com a lei, o objetivo da LGPD é proteger os direitos fundamentais de liberdade e privacidade dos brasileiros quanto aos seus dados pessoais, inclusive nos meios digitais, protegendo dados pessoais de pessoas naturais. Aplicando-se a todo território nacional, a lei inclui tanto pessoas jurídicas de direito público quanto privado. Cardoso (2020) enfatiza, entretanto, que a LGPD não é a primeira a tratar do assunto no país. O juiz federal afirma que a temática da proteção dos dados é anterior ao alargamento do acesso à internet e ao uso de meios digitais para fins comerciais.

> Assim, a LGPD não é a primeira lei no Brasil que regula e protege os direitos dos titulares de dados pessoais, sendo que a temática é objeto de atenção do Legislativo há alguns anos, mesmo antes do enquadramento jurídico da matéria em sua amplitude atual (CARDOSO, 2020).

Da mesma forma, Garcia et al. (2020) citam a Constituição Federal (CF/88), o Código de Defesa do Consumidor (Lei n. 8.078/1990), o Decreto do Comércio Eletrônico (Lei n. 9.507/1997), a Lei de Acesso à Informação (Lei n. 12.527/2011), a Lei do *Habeas Data* (Decreto n. 7.962/2013), o Marco Civil da Internet (Lei n. 12.965/2014), como textos antecessores à LGPD, mas que, de alguma forma regem o direito à privacidade e dão proteção jurídica aos dados pessoais.

Como tutela ao direito da personalidade da pessoa natural, o CC – Lei n. 10.406 – dispõe conteúdo em defesa da dignidade da pessoa humana, na forma da lei, intransmissíveis e irrenunciáveis, em seus arts. 11 e 21 (como já apresentado). De forma indireta, o próprio Código Tributário Nacional (CTN; Lei n. 5.172, de 25 de outubro de 1966) veda à Fazenda (e seus servidores) que divulguem informações acerca da situação econômica/ financeira ou sobre as negociações ou atividades dos contribuintes. Conforme Art. 198, Lei Complementar n. 104, de 10 de janeiro de 2001:

> Art. 198. Sem prejuízo do disposto na legislação criminal, é vedada a divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades.

Cardoso (2020) tece um rápido resumo histórico e cronológico sobre as leis e normas que antecederam a promulgação da LGPD, oportunamente apresentado. Primeiramente, o autor destaca que "[...] o Código de Defesa do Consumidor (Lei nº 8.078/90) contém as primeiras normas sobre a regulação da formação dos bancos de dados no Brasil", sendo, portanto, uma das primeiras leis brasileiras a tratar da matéria dos dados, datada de 1990. Sobre o Código de Defesa do Consumidor (CDC), Cardoso (2020) defende que as relações jurídicas estabelecidas entre pessoas, de ordem natural ou empresarial, são perpassadas por dados.

> As relações jurídicas mantidas entre uma pessoa (natural ou jurídica, de direito público ou privado) que realiza atividades de tratamento de dados e outra pessoa (natural) titular desses dados, em regra, enquadra-se no conceito de relação de consumo submetida ao microssistema do Código de Defesa do Consumidor (CARDOSO, 2020, s/p).

Além do CDC, outra legislação anterior à LGPD, e que também trata de dados, é a LAI – amplamente discutida na seção 2.2 e 2.3. A LAI destaca-se, representa um marco significativo, pois permite a fiscalização de processos financeiros, administrativos, fiscais e quaisquer outras atividades realizadas pelo poder público mas que sejam de interesse coletivo. Assim, a LAI obriga a Administração Pública a dar publicidade de seus atos administrativos, possibilitando a fiscalização, de ações dos poderes Executivo, Legislativo e Judiciário.

Através dos breves apontamentos sobre os mecanismos legais antecessores à LGPD, Cardoso (2020) enfatiza o diálogo das fontes, isto é, as outras legislações que se entrecruzam nos artigos da Lei Geral. Garcia et al. (2020) afiançam que a LGPD, inspirada na RGPD, é a mais específica e exclusiva lei e, por isso, tem principal relevância.

É importante destacar que a LGPD é um marco legal de grande impacto, atingindo tanto as instituições privadas como as públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação, por qualquer meio, que envolva o tratamento de informações classificadas como dados pessoais de pessoa natural ou jurídica.

4 DIREITO COMPARADO: LGPD E RGPD

Esclarece-se, primeiramente, que a análise comparativa entre os modelos jurídicos exige, por finalidade, clareza metodológica. Por essa razão é que se adota o método funcional de direito comparado, apresentada por Cury (2014, p. 178), onde se procura respeitar o núcleo desse método, que pressupõe a compatibilidade do que se compara, isto é, de elementos que preencham as mesmas funções jurídicas. Uma das formas de demonstrar as semelhanças e diferenças (comparar, portanto) duas ou mais regras é por meio da apresentação de quadros – o que será feito.

No Brasil, ainda em 2010, houve a primeira consulta pública sobre a versão do anteprojeto de lei que, mais tarde, seria a LGPD. Em 14 de agosto de 2018, em complementação ao Marco Civil da Internet, a Lei n. 13.709 foi aprovada, sob a alcunha de Lei Geral de Proteção de Dados, entrando em vigência em 18 de setembro de 2020 (PINHEIRO, 2021). Da mesma forma, a Medida Provisória (MP) n. 869/18, convertida na Lei n. 13.853/2019, estabeleceu a Autoridade Nacional de Proteção de Dados (ANPD). No entendimento de Pinheiro (2021), a LGPD não é perfeita, cabendo à ANPD esclarecer alguns pontos. Mendes (2019, p. 35) ressalta que:

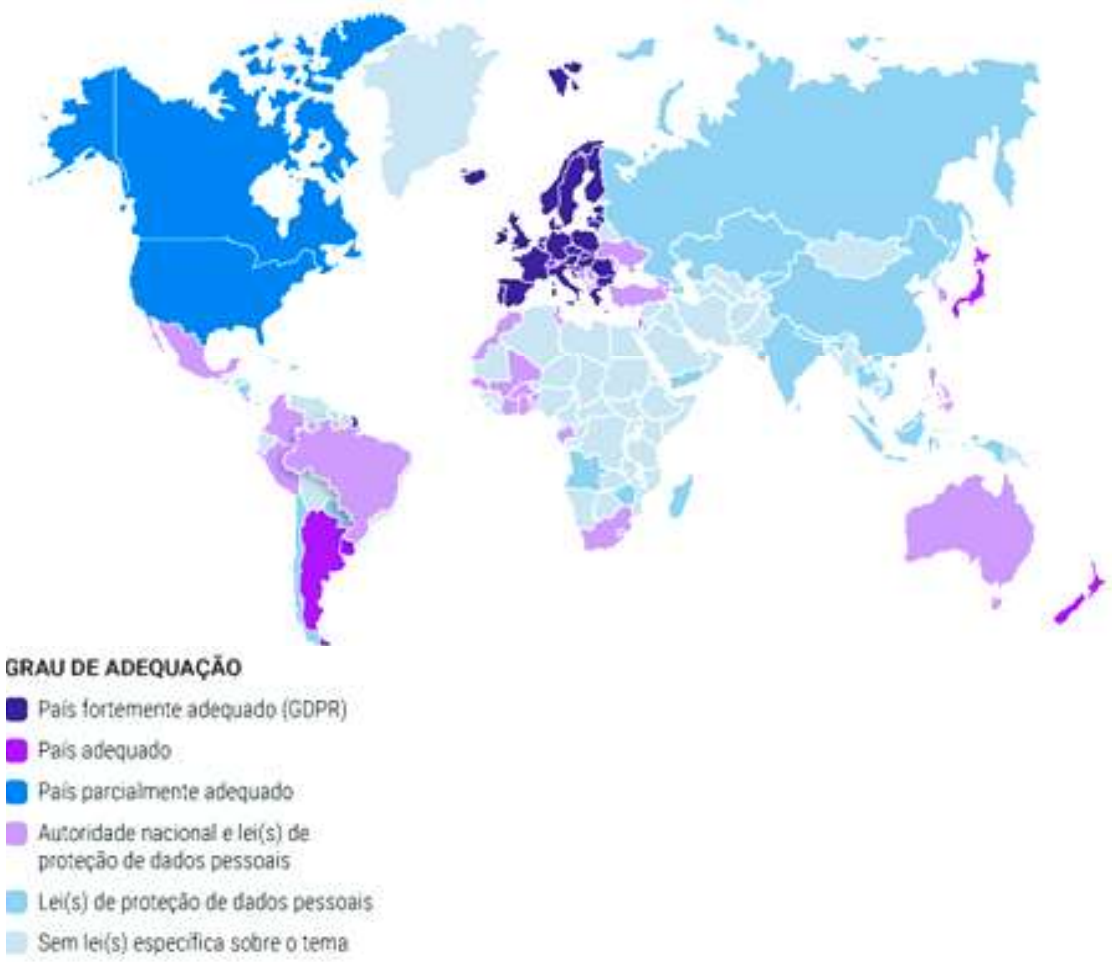
> A disciplina da proteção de dados pessoais emerge no âmbito da sociedade de informação, como uma possibilidade de tutelar a personalidade do indivíduo, contra os potenciais riscos a serem causados pelo tratamento de dados pessoais. A função não é a de proteger os dados per se, mas, sim, a pessoas que é titular desses dados.

Elucida-se que o Regulamento Geral de Proteção de Dados (RGPD), aprovado em 2016, entrou em vigor em maio de 2018 (em substituição a Diretiva de Proteção de Dados, de 1995), sendo o principal regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na UE e Espaço Econômico Europeu. A UE é um bloco econômico de natureza supranacional, com um modelo de Direito Comunitário, com escopo territorial abrangendo, atualmente, 27 Estados membros – Alemanha, Áustria, Bélgica, Bulgária, Chipre, Croácia, Dinamarca, Eslováquia, Eslovênia, Espanha, Estônia, Finlândia, França, Grécia, Holanda, Hungria, Irlanda, Itália, Letônia, Lituânia, Luxemburgo, Malta, Polônia, Portugal, República Tcheca, Romênia, Suécia (o Reino Unido já não faz parte da UE).

Ainda, importa trazer o mapa apresentado pelo Serpro (2022a) [3], que demonstra a abrangência das leis da proteção de dados pessoais no mundo (figura 1).

3 Maior empresa pública de Tecnologia da Informação do mundo, responsável por mais de 90% das soluções digitais do Estado brasileiro e líder do mercado nacional de TI. O Serpro tem compromisso com a segurança e garantia da revolução tecnológica brasileira e é protagonista na LGPD, auxiliando o país na adequação aos princípios da lei (SERPRO, 2022a).

Figura 1 – Mapa da abrangência de leis de proteção de dados pessoais: mundo



Fonte: Serpro (2022b).

Wachowicz (2020) inicia sua análise dos princípios jurídicos de tratamento de dados pessoais comparando a LGPD e a RGPD, pois afirma que a análise simultânea e comparativa dos ordenamentos brasileiro e europeu é justificável, em razão da similaridade dos dois textos. Tal similaridade não é, obviamente, acidental, como já comentado. O Brasil – em decorrência das exigências europeias em manter negociações comerciais apenas com países que, da mesma forma que eles, protegessem os dados pessoais legalmente – editou uma legislação inspirada no modelo europeu, a exemplo de outros países. A promulgação da RGPD "[...] ocasionou um 'efeito dominó', visto que passou a exigir que os demais países e as empresas que buscassem manter

relações comerciais com a UE também deveriam ter uma legislação de mesmo nível [...]" (PINHEIRO, 2021, s/p). Segundo Iramina (2020, p. 92):

> Considerando que empresas geralmente operam extraterritorialmente, a convergência global das normas que regulam a proteção de dados tem-se mostrado fundamental, não só para facilitar o fluxo de dados e, consequentemente, o comércio e a cooperação entre as organizações e as autoridades públicas, mas também para aumentar o nível de proteção de dados pessoais em todo o mundo. Não por acaso, grande parte das mais recentes legislações de proteção de dados são inspiradas no Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, em vigor desde maio de 2018, e, portanto, apresentam características similares, como: 1) legislação geral e abrangente (em vez de normas setoriais); 2) proteção de direitos individuais; 3) autoridade supervisora independente.

Neste mesmo sentido, para corroborar tais afirmações, Almeida e Soares (2022, p. 30) afirmam que:

> No Brasil, em 14 de agosto de 2018, entrou em vigor a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, publicada no Diário Oficial da União (D.O.U.) em 15/8/20183 . A Lei de Proteção de Dados Pessoais (LPD), buscou no então recente Regulamento Geral de Proteção de Dados (*General Data Protection Regulation* – GDPR), sigla em inglês da União Europeia, orientações para a elaboração de normas para a proteção dos dados pessoais, de indivíduos [...].

Uma observação a ser feita diz respeito à divisão de ambas as leis. A LGPD está dividida em 10 capítulos, com 65 artigos, já a RGPD possui 11 capítulos, com 99 artigos. Sendo assim, a lei nacional brasileira é mais enxuta, deixando alguns aspectos em aberto, como o caso dos prazos de cumprimento de decisões – a RGPD fixa 72 horas, a LGPD prevê prazo razoável. Porém, muito embora existam diferenças, a LGPD e o GDPR têm muito mais pontos de convergência do que de divergência.

Sob a perspectiva regulatória, ambas as leis adotam uma abordagem estratégica para o tratamento de dados pessoais, incentivando e regulamentando as boas práticas de privacidade das empresas e instituições. Outras semelhanças gerais são: "[...] a adoção de uma legislação abrangente

sobre o tema, o estabelecimento de direitos fundamentais para os titulares dos dados e a criação de uma autoridade supervisora independente" (IRAMINA, 2020, p. 93). Abaixo explica-se algumas comparações.

Primeiramente, ambos os regulamentos destacam a importância de estabelecer uma estrutura sólida de governança em relação à privacidade e à proteção de dados. Isso inclui a atribuição de responsabilidades a indivíduos específicos, como o Encarregado de Proteção de Dados (DPO), que atua como ponto focal para questões de privacidade. Além disso, ambas as leis enfatizam a importância de disseminar a cultura de proteção de dados por toda a organização, com a designação de outros responsáveis pela privacidade e a promoção de comunicações regulares entre essas partes.

No que diz respeito ao tratamento de dados pessoais, tanto o RGPD quanto a LGPD ressaltam a necessidade de manter um inventário detalhado desses dados, bem como fluxogramas que indicam os fluxos de dados, especialmente em contextos transfronteiriços. Ambos os regulamentos também enfatizam a importância da adoção de medidas de segurança adequadas, incluindo a criptografia e a restrição de acesso, como parte integrante da proteção dos dados pessoais.

A elaboração e manutenção de políticas de privacidade e proteção de dados são igualmente abordadas por ambos os regulamentos. Ambas as leis exigem que as organizações documentem as bases legais para o tratamento de dados e integrem considerações éticas, como códigos de conduta, no tratamento dessas informações sensíveis.

A importância do treinamento e da conscientização também é uma convergência notável. Ambos os regulamentos reconhecem a necessidade de treinamentos regulares em privacidade e proteção de dados para os funcionários, bem como a integração desses princípios nos treinamentos operacionais, como recursos humanos e centrais de atendimento.

No âmbito do tratamento de dados por terceiros, o RGPD e a LGPD concordam sobre a importância de manter políticas claras para terceirizados e conduzir due diligencie em relação às práticas de privacidade e proteção de dados dessas partes.

Além disso, ambos os regulamentos enfatizam a importância de responder de maneira eficaz às solicitações e reclamações dos titulares de dados, incluindo pedidos de acesso, retificação, exclusão e portabilidade.

Por fim, tanto o RGPD quanto a LGPD destacam a necessidade de monitorar e atualizar constantemente as práticas operacionais em relação à privacidade de dados, bem como a importância de gerenciar adequadamente incidentes de segurança e violações de dados.

Em resumo, o comparativo entre o RGPD e a LGPD revela uma série de semelhanças notáveis nas atividades de gerenciamento de privacidade e proteção de dados. Essas convergências ressaltam a preocupação global com a proteção de dados pessoais, independentemente do contexto jurisdicional, e enfatizam a importância de uma abordagem abrangente para garantir a conformidade e proteger os direitos dos indivíduos em relação aos seus dados pessoais.

O que se disse até aqui basta, por si só, a fim de demonstrar que a proteção de dados pessoais é hoje um domínio em que, a par da circulação de modelos jurídicos através das fronteiras – de que o RGPD e a LGPD constituem um exemplo paradigmático –, deparamos também com conceções muito diversas nos sistemas jurídicos nacionais; e em que a comparação jurídica, permitindo descortinar as semelhanças e as diferenças entre esses sistemas jurídicos e explicá-las por apelo aos seus fundamentos e origens, constitui um instrumento essencial para a sua compreensão.

5 A PROTEÇÃO JURÍDICA DE DADOS PESSOAIS EM PERSPECTIVA: ESTADOS UNIDOS E JAPÃO

Por sua relevância econômica e tecnológica, tanto nos Estados Unidos (EUA) quanto no Japão a temática da proteção jurídica de dados pessoais é importante e amplamente discutida há décadas. Apresentam-se informações pertinentes e traçam-se divergências e convergências entre as leis dos EUA e do Japão com a RGPD e LGPD, da UE e Brasil, respectivamente.

5.4.1 ESTADOS UNIDOS

Os Estados Unidos da América (EUA) são, mesmo em meio às muitas incertezas do cenário global pós pandemia, a maior economia do mundo e o

terceiro país com maior população. Seu produto interno bruto (PIB) voltou a crescer no último trimestre de 2022 (2,6%) e o dólar (moeda corrente norte americana) continua se fortalecendo (IPEA, 2022).

Na década de 1970, o país foi marcado pelo caso do *National Data Center*. A proteção jurídica de dados pessoais foi posta em debate após ser proposta a unificação das bases de dados e o uso das TICs para armazenamento e processamento de grande volume de dados pessoais. Parte da população norte americana se opôs à centralização de conteúdos e o congresso nacional acabou não apoiando a criação do *National Data Center* até que fosse provada a proteção da privacidade e garantida proteção aos cidadãos.

Nenhuma lei foi criada após este episódio e as leis de proteção de dados pessoais nos Estados Unidos ainda são fragmentadas e liberais, diferentemente do que ocorre, em particular, nos Estados-Membros da União Europeia e no Brasil, que apresentam uma regulamentação de índole fortemente abrangente, pormenorizada e protetora. A proteção jurídica dos dados nos EUA é, portanto, contrastante com a praticada e imposta pela LGPD e RGPD.

Segundo Cardoso (2020), nos EUA, a legislação que trata sobre a temática da proteção dos dados conta com uma série de leis e não com uma lei geral, como é o caso do Brasil e da União Europeia. Detalha-se, convenientemente, que, tanto no Brasil quanto na UE, a noção de dados pessoais sujeitos a proteção é muito ampla, entendidos como "toda a informação relativa a uma pessoa singular identificada ou identificável", porém a noção norte-americana, muito mais restritiva, confere particular ênfase à proteção da privacidade dos indivíduos perante as agências públicas – há o *Privacy Act of 1974*, cujas normas limitam a coleta de dados dos cidadãos pelo governo.

Assim, enquanto no Brasil e nos países europeus a privacidade é essencialmente uma exigência da dignidade da pessoa humana, "[...] a salvaguardar em particular perante entidades privadas, os norte-americanos veem antes nela uma expressão da liberdade individual, primariamente ameaçada pelo Estado" (WACHOWICZ, 2020, p. 14).

Ainda, RGPD e LGPD baseiam-se no princípio do consentimento, enquanto no Direito norte-americano, o recente aprovado *California Consumer Privacy Act* (Lei de Privacidade do Consumidor da California) limita-se a acolher nesta matéria um direito de *opting-out* (optar para sair), nos termos do qual o consumidor pode recusar a possibilidade de venda a terceiros da sua informação pessoal.

O direito ao esquecimento – tão caro ao RGPD e à LGPD – também não encontra qualquer correspondência no Direito norte-americano. Encontra-se, no entanto, e de forma contrária, que o tratamento de dados alheios faz parte do direito à liberdade de expressão, defendido como fulcral e reiteradamente blindado por tribunais federais estadunidenses, protegido pela 1ª Emenda à Constituição norte-americana.

Há, porém, tramitando desde 30 de dezembro de 2022 (após ser aprovado pelo Comitê de Energia e Comércio da Câmara em 21 de junho de 2022) a *American Data Privacy and Protection Act* (ADPPA), que seria uma lei federal abrangente de proteção de dados e substituiria a maioria das leis estaduais que regem a privacidade do cidadão estadunidense. A promulgação da ADPPA se aplicaria amplamente a organizações e empresas que operam nos Estados Unidos. Algumas das principais definições incluem:

Consentimento Expresso Afirmativo: Refere-se a um ato claro e inequívoco por parte de um indivíduo, indicando sua autorização livre e específica para a coleta ou uso de dados após ter sido informado sobre a prática. Autenticação: Define o processo de verificação da identidade de um indivíduo ou entidade, visando garantir a segurança dos dados.

Informações Biométricas: Compreende dados gerados pelo processamento tecnológico das características únicas de um indivíduo, como impressões digitais, varreduras de íris ou voz. No entanto, certos tipos de informações, como fotos ou gravações de áudio/vídeo, não se enquadram nessa categoria.

Entidade Coberta: Refere-se a qualquer entidade ou pessoa que determine os propósitos e métodos de coleta, processamento ou transferência de dados. Isso exclui indivíduos atuando em um contexto não comercial.

Dados Cobertos: Engloba informações que identificam ou estão vinculadas a um indivíduo ou dispositivo. Isso também inclui dados derivados e identificadores únicos persistentes.

Dados Sensíveis Cobertos: Define categorias específicas de informações sensíveis, como informações de saúde, números de conta financeira, informações biométricas e dados genéticos.

Provedor de Serviços: É uma pessoa ou entidade que coleta, processa ou transfere dados em nome de uma entidade coberta, visando executar um serviço ou função sob a direção dessa entidade.

Entidade de Coleta de Terceiros: Refere-se a uma entidade coberta cuja receita principal deriva do processamento ou transferência de dados, mesmo que esses dados não tenham sido coletados diretamente dos indivíduos afetados.

Danos Potenciais: Refere-se aos riscos de dano relacionados a indivíduos menores de 17 anos, discriminação com base em características protegidas (como raça ou religião), acesso ou restrições a serviços como moradia, educação e saúde, além de disparidades resultantes desses fatores.

Essas definições formam a base da ADPPA e são cruciais para garantir a proteção dos direitos individuais em um ambiente cada vez mais digitalizado.

Ao se visitar o texto completo do projeto de Lei, introduzido em 30 de dezembro de 2022 (Relatório nº 117-669), observa-se que o principal objetivo da proposta é fornecer aos consumidores direitos fundamentais de privacidade de dados, criar mecanismos de supervisão fortes e estabelecer uma aplicação significativa.

Esclarece-se que, embora a definição de entidade coberta seja inegavelmente ampla, a ADPPA identifica vários tipos diferentes de entidades com obrigações ou isenções adicionais. Para certas obrigações, as entidades abrangidas são divididas por "impacto" (ou seja, receita global anual e número de titulares de dados afetados pelas operações da entidade) e "relação com o titular dos dados" (por exemplo, relações diretas, com terceiros ou prestadores de serviços). A título de exemplo, uma entidade "grande" é definida como aquela com receita bruta anual de pelo menos US$ 250 milhões e que coletou dados cobertos em mais de 5 milhões de indivíduos ou dispositivos ou coletou dados confidenciais cobertos de mais de 100.000 indivíduos ou dispositivos.

É importante ressaltar que tanto os dados dos funcionários quanto os dados disponíveis publicamente estão excluídos desta definição. Certos tipos de dados cobertos são definidos como dados cobertos confidenciais, que incluiriam identificadores do governo (como carteira de motorista ou números de seguro social), bem como informações «tradicionalmente» confidenciais relacionadas a saúde, geolocalização, finanças, credenciais de login, raça, e história ou identidade sexual. Os dados confidenciais também podem incluir outras categorias, como dados de exibição de televisão, imagens íntimas e "informações que identificam as atividades online de um indivíduo ao longo do tempo ou em sites ou serviços online de terceiros".

Ainda, uma entidade de coleta de terceiros seriam obrigadas a fornecer aos consumidores um aviso de sua atividade e se registrar na *Federal Trade Commission* [4] (FTC) se processarem dados pertencentes a mais de 5.000 indivíduos ou dispositivos que possam ser razoavelmente vinculados a um indivíduo, bem como fornecer aos consumidores a oportunidade de exigir que tal entidade exclua os dados cobertos de um consumidor.

Resta apresentar as regras propostas para a supervisão de Inteligência Artificial (IA) e o uso de algoritmos [5]. A seção 207 (Direitos Civis e Algoritmos) assevera que entidades ou provedores de serviços cobertos "não podem coletar, processar ou transferir dados cobertos de maneira que discrimine ou torne indisponível o aproveitamento igual de bens ou serviços com base em raça, cor, nacionalidade, sexo ou deficiência". Ao contrário da maioria das leis estaduais de privacidade existentes, a Seção 207 da ADPPA iria um passo além, exigindo que as empresas avaliassem certas ferramentas de IA e submetessem essas avaliações à FTC.

Por enquanto, espera-se e observam-se vários movimentos relutantes e de oposição à promulgação da ADPPA, inclusive de apoiadores de mudanças no sentido de viabilizar e flexibilizar a cada Estado o uso ou não das regras legais expostas. A própria California afirma que a CCPA dá mais proteção aos consumidores e mais controle de suas informações do que o texto do projeto de lei da ADPPA.

5.4.2 JAPÃO

Atualmente, o Japão é a terceira maior economia mundial (considerando o PIB nominal) e o décimo primeiro país com maior população no mundo, sendo uma das mais antigas democracias da Ásia (com parlamento bicameral e uma monarquia constitucional com um imperador). Além disso – e um dos

4 Comissão Federal de Comércio

5 O projeto de lei define um algoritmo como: um processo computacional que usa aprendizado de máquina, processamento de linguagem natural, técnicas de inteligência artificial ou outras técnicas de processamento computacional de complexidade semelhante ou maior que toma uma decisão ou facilita a tomada de decisão humana com relação aos dados, inclusive para determinar o fornecimento de produtos ou serviços ou para classificar, ordenar, promover, recomendar, ampliar ou determinar de forma semelhante a entrega ou "exibição de informações a um indivíduo".

fatores que mais sustenta a relevância deste país quando o assunto é acesso à informação e direito à privacidade e proteção jurídica de dados pessoais – o Japão é o país líder em inovações tecnológicas. Ainda, importa ressaltar que, mesmo após sofrer influência do sistema jurídico do ocidente (por volta de 1858), as regras jurídicas japonesas são conhecidas como pouco flexíveis – o que reflete a cultura moral rígida e o código de honra que molda e fundamenta as relações nipônicas (o *giri*).

A Lei de Proteção de Informações Pessoais do Japão (LPIP-JP) foi promulgada em 2003 e sofreu reforma em 2013 e ampla mudança em 2017 (GREENLEAF, 2014), que, inclusive, estabeleceu revisão trianual obrigatória (a mais recente foi em 2020). Até 2011, segundo Miyashita (2011, p. 233 [tradução nossa]):

> As regras legais para os mecanismos de aplicação são muito particulares no Japão e diferem da forte aplicação da lei nos países europeus. No entanto, é extremamente importante entender que uma violação de dados no Japão significa a ruptura da confiança social e do relacionamento íntimo com os clientes. No Japão, o risco de perda de confiança social e reputação empresarial é considerado muito mais significativo do que pagar uma multa. Assim, as empresas geralmente seguem as diretrizes emanadas dos ministérios governamentais, e algumas também adotam suas próprias diretrizes [...].
>
> [6]

De acordo com Greenleaf (2014), as reformas ocorreram, principalmente, para sanar as fragilidades da lei japonesa e cumprir as expectativas internacionais sobre a privacidade dos dados pessoais no ciberespaço. A Comissão Europeia lançou comunicado, em janeiro de 2017, que confirmou a modernização da legislação do Japão, tornando o regime abrangentes em matéria de proteção de dados (COMISSÃO EUROPEIA, 2017). Em Decisão de Execução (UE) 2019/419, de 23 de janeiro de 2019, a LPIP-JP foi considerada compatível com a RGPD (COMISSÃO EUROPEIA, 2019).

A LPIP-JP é aplicada a todos os Controladores de Dados Pessoais

6 The legal rules for enforcement mechanisms are very particular in Japan, and differ from the strong enforcement of the law in European countries.33 However, it is crucially important to understand that a data breach in Japan means the disruption of social trust and the intimate relationship with customers. In Japan, the risk of loss of social trust and business reputation is regarded as much more significant than paying a fine. Thus, businesses generally follow the guidelines issued by government ministries, and some also adopt their own guidelines […].

(CDP), sejam pessoas físicas ou jurídicas, e modificada pela Comissão de Proteção de Informações Pessoais do Japão (CPIP-JP).

Destacam-se algumas definições, pois são relevantes para fim de comparação com a RGPD e LGPD. Segundo Hounslow (2021), na LPIP-JP, em suas diretrizes gerais, há a definição de:

- Informações pessoais: Informações sobre pessoa que resida no Japão. Nessa categoria, incluem-se 'códigos de identificação pessoal', tais como: itens como caracteres, números, símbolos e/ou outros códigos para uso do computador que representam certas características físicas pessoais especificadas (como sequências de DNA, aparência facial, impressões digitais e palmares), e que são suficientes para identificar um indivíduo específico, bem como determinados números de identificação, como os de passaportes, carteiras de habilitação e cartões de residente e os números de identificação individual da previdência social.
- Dados pessoais: Informações pessoais contidas em um banco de dados.
- Dados sensíveis: informações pessoais relacionadas a questões como: raça, credo, religião, deficiência física ou mental, registros médicos, tratamento médico e farmacológico, prisão, detenção ou processo criminal (seja adulto ou jovem), ou vitimização criminal.
- Titular dos dados: o indivíduo que é o titular das informações pessoais.

A comparação entre a Lei Geral de Proteção de Dados (LGPD) do Brasil e a Lei de Proteção de Informações Pessoais (LPIP-JP) do Japão revela tanto convergências quanto divergências cruciais em suas abordagens de proteção de dados:

No que diz respeito à Autoridade de Proteção de Dados, as duas legislações diferem substancialmente. Enquanto a LGPD brasileira estabelece uma autoridade não autônoma e não independente, responsável por fiscalizar e implementar a lei, a LPIP-JP japonesa adota uma abordagem autônoma e independente, onde a Comissão de Proteção de Informações Pessoais possui a autoridade de operar sem interferências, sob a direção do Primeiro-Ministro.

A definição de "Titulares de Dados" também possui nuances contrastantes. Na LGPD, um "titular" é uma pessoa natural relacionada aos dados pessoais. Já na LPIP-JP, o termo refere-se a um indivíduo específico identificável por meio de informações pessoais, tornando a abordagem japonesa mais direcionada à identificação singular.

O direito à informação é abordado de forma similar, porém com enfoques distintos. A LGPD preza pela transparência através de informações claras sobre o tratamento dos dados. Por outro lado, a LPIP-JP exige que um PIHBO forneça tópicos específicos prontamente para que o titular esteja ciente, destacando a ênfase japonesa na pronta resposta a solicitações.

No âmbito do direito de acesso, ambas as leis visam assegurar que os titulares possam consultar seus dados pessoais. Enquanto a LGPD enfatiza o "livre acesso" e a facilidade de consulta, a LPIP-JP especifica que o titular pode exigir a divulgação de dados pessoais retidos por um PIHBO, seguindo procedimentos definidos pela Comissão de Proteção de Informações Pessoais.

O direito à limitação do tratamento também apresenta discrepâncias notáveis. A LGPD enfatiza a anonimização, bloqueio ou eliminação de dados desnecessários ou tratados inadequadamente. Em contrapartida, a LPIP-JP estabelece várias cláusulas que exigem o consentimento prévio para o tratamento de informações pessoais, e permite que o titular exija correções, adições ou exclusões quando necessário.

Essas divergências e convergências evidenciam as diferentes abordagens adotadas pelo Brasil e Japão na proteção de dados e informações pessoais. Cada legislação reflete os contextos e valores específicos de cada país, contribuindo para a moldagem das estruturas regulatórias de proteção de dados. Adaptado de Marques (2021).

Convergência e divergência entre LGPD e LPIP-JP delineiam as distintas abordagens adotadas pelo Brasil e Japão na proteção de dados e informações pessoais, enfatizando as variações regulatórias e as similaridades que moldam as estruturas legais de ambos os países. Adaptado de Marques (2021).

A evolução da proteção jurídica das informações pessoais no Japão fez com que o país esteja considerado como zona em *compliance* (confiança) no tratamento de dados pela UE. Como se pode observar na figura 1, o Japão é reconhecido pela UE como um dos únicos países asiáticos considerados adequado para ser zona de trânsito seguro de dados. Tanto o Japão quanto

a Coreia do Sul são reconhecidos pela UE em relação à confiança de procedimentos em tratamentos de dados, porém o Japão é considerado como zona de tratamento de alto nível no que se refere a dados, o que cria um sistema de livre trânsito de dados, em que as barreiras burocráticas não são necessárias.

Assim, após avaliação de adequação, a UE, em 2019, afirmou que a relação em Japão e UE é a maior área de fluxo de dados seguros do mundo e colocou em vigor o Acordo de Parceria Econômica UE-Japão, contando com fluxo livre de dados entre empresas de ambos os países.

6 CONCLUSÃO

A Lei Geral de Proteção de Dados (LGPD) no Brasil e a proteção jurídica de dados pessoais ao redor do mundo são reflexos das rápidas inovações tecnológicas e da necessidade de estabelecer diretrizes para garantir a privacidade e a segurança dos indivíduos no ciberespaço.

Ao comparar a LGPD com o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, podemos observar semelhanças e diferenças nas abordagens adotadas para proteger os dados pessoais. Enquanto a LGPD é uma lei brasileira que busca estabelecer diretrizes claras e fiscalização através da Autoridade Nacional de Proteção de Dados (ANPD), o RGPD abrange toda a União Europeia e possui regulamentações mais abrangentes.

Nos Estados Unidos, a proteção jurídica de dados pessoais é abordada por leis setoriais e estaduais, como o California Consumer Privacy Act (CCPA) e o General Data Protection Regulation (GDPR) na União Europeia. Embora não exista uma lei federal de proteção de dados abrangente, o país está cada vez mais discutindo a implementação de regulamentações mais abrangentes nesse sentido.

No Japão, a Lei de Proteção de Informações Pessoais (LPIP-JP) tem evoluído ao longo dos anos, acompanhando as inovações tecnológicas do país. O Japão é conhecido por ser líder em inovações tecnológicas e por ser considerado uma zona em compliance no tratamento de dados pela União Europeia, o que facilita o livre trânsito de dados entre o país e a UE.

Em conclusão, a proteção de dados pessoais é uma necessidade global

que está sendo abordada de diferentes maneiras em diferentes países. A LGPD no Brasil, juntamente com as regulamentações internacionais, visa garantir a privacidade dos indivíduos e o uso adequado de suas informações. Compreender as abordagens adotadas no Brasil, nos Estados Unidos e no Japão nos ajuda a identificar melhores práticas e aprimorar as políticas de proteção de dados em âmbito nacional e internacional.

REFERÊNCIAS

ALMEIDA, S. do C. D. de; SOARES, T. A. Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital *Perspectivas em Ciência da Informação*, v. 27, n. 3, p. 26-45, jul/set 2022.

ARAÚJO, V. S.; GOMES, M. L. *Inteligência Artificial.* E aplicabilidade prática no Direito. Conselho Nacional de Justiça, 2022.

BARROSO, L. R. *Curso de Direito Constitucional Contemporâneo.* 10. ed. São Paulo: Saraiva, 2022. E-book.

BOFF, S. O.; FORTES, V. B. A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil. *Seqüência* (Florianópolis), n. 68, p. 109-127, jun. 2014.

BORTALI, H. P. *Limites da atividade do provedor*: o gerenciamento de dados e a responsabilidade sobre conteúdo de terceiros. 2020. 134 f. Dissertação (Mestrado em Direito) - Programa de Estudos Pós-Graduados em Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2020.

BRASIL. *Código civil de 2002*. Lei Federal nº 10.406, de 10 de janeiro de 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em 20 jun. 2022.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 13 jun. 2021.

BRASIL. *Lei de acesso à informação. Lei Federal nº 12.527*, de 18 de novembro de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em 3 maio 2022.

BRASIL. *Lei dos cartórios.* Lei Federal nº 8.935, de 18 de novembro de 1994. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8935.htm>. Acesso em: 10 jun. 2022.

BRASIL. *Lei geral de proteção de dados pessoais (LGPD).* Lei Federal nº 13.709, de 14 de agosto de 2018. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei /l13709.htm. Acesso em 12 jan. 2022.

BRASIL. *Lei n. 9.492,* de 10 de setembro de 1997. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9492.htm>. Acesso em: 28 fev. 2023.

CARDOSO, O. V. *Introdução à Lei Geral de Proteção de Dados Pessoais*. E-book, 2020.

CASTELLS, M. A *sociedade em rede*. A era da informação: economia, sociedade e cultura. São Paulo: Paz e Terra, 2011.

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

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

CONSELHO DA JUSTIÇA FEDERAL. Enunciado 531. Disponível em: <

COSTA, I.; DALLEDONE, R. Direito à privacidade X Direito à informação: novos aportes para o debate brasileiro. *Revista Jurídica da Escola Superior do Ministério Público de São Paulo*, v. 18, n. 2, 2020, p. 131-145.

CRESWELL, J. W.; CRESWELL, J. D. *Projeto de pesquisa: métodos qualitativo, quantitativo e misto*. 5. ed. Porto Alegre: Artmed, 2021.

CURY, P. M. N. *Métodos de Direito Comparado:* desenvolvimento ao longo do século XX e perspectivas contemporâneas. Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD). UNISINOS. Julho-setembro/2014, p. 176-185.

DA SILVA, S. de A. A. et al. *Herança da informação digital e direito ao esquecimento em redes sociais on-line*: uma revisão sistemática de literatura. Em Questão, Porto Alegre, v. 26, n. 1, p. 375-401, jan/abr. 2020.

DIÁRIO OFICIAL. PORTARIA ANPD n. 35, de 4 de novembro de 2022. *Torna pública a Agenda Regulatória para o biênio 2023-2024. 2022*. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885>. Acesso em: 27 fev. 2023.

EDUCACAO, S. *Lei Geral de Proteção de Dados (LGPD) e Marco Civil da Internet*. São Paulo:

GARCIA, L. R. *Lei Geral de Proteção de Dados Pessoais (LGPD):* guia de implantação. São Paulo: Blucher, 2020.

GÓIS, J. A. de O. *A intimidade e a vida privada em face de biografias não autorizadas.* Avanços da esfera pública sobre a esfera privada. e-Book: Dialética, 2020.

GREENLEAF, G. *Asian Data Privacy Laws:* Trade & Human Rights Perspectives. Oxford: Oxford University Press, 2014. E-book/Kindle Edition.

GRESSLER, I.C.; BACHINSKI, F. L.; SILVA, R. L. *A divulgação indevida de informações pessoais em site de universidade gaúcha*: resposta jurisdicional entre a óptica constitucional e os princípios da lei n. 13.709/2018. X Congresso Internacional de Direito e Contemporaneidade: mídia e direitos da sociedade em rede. UFSM, 2019.

HARARI, Y. N. *SAPIENS* – Uma Breve História da Humanidade. L&PM, 2017.
HOUNSLOW, D. Japan - Data Protection Overview. OneTrust – Data Guidance, 2021. Disponível em: <https://www.dataguidance.com/notes/japan-data-protection-overview. Acesso em: 13 de nov. de 2022.

INSTITUTO DE PROTESTO – IEPTB-BR. *Política de privacidade e cookies.* Versão 1.0. 2022. Programa de governança em privacidade e proteção de dados pessoais. Disponível em: <https://www.protestodetitulos.org.br/arquivos/politica-privacidade.pdf>. Acesso em 10 dez. 2022.

IRAMINA, A. RGPD v. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. *Revista de Direito, Estado e Telecomunicações, Brasília*, v. 12, n. 2, p. 91-117, outubro de 2020.

PINHEIRO, P. *P. Proteção de Dados Pessoais.* 3. ed. São Paulo: Saraiva Educação, 2021.

WACHOWICZ, M. (org). *Proteção de dados pessoais em perspectiva:* LGPD e RGPD na ótica do direito comparado. Curitiba, PR: Gedai, 2020.