doi.org/10.51891/rease.v11i12.23524

COMPARAÇÃO ENTRE A LEI DE PROTEÇÃO DE DADOS BRASILEIRA (LGPD) E A LEGISLAÇÃO DE PROTEÇÃO DE DADOS DOS ESTADOS UNIDOS: ANÁLISE COM ENFOQUE NOS ESTUDOS DE DANILO DONEDA, BRUNO BIONI E PERSPECTIVAS ATUAIS

André Luiz Santiago Jabur[1]
Lauryenne Lopes de Oliveira[2]
Loren Vânia Lopes de Oliveira[3]
Ramon Costa de Faria[4]
Sérgio Ricardo Moreira de Souza[5]

RESUMO: Este trabalho propõe uma análise abrangente e atualizada da Lei Geral de Proteção de Dados (LGPD) do Brasil e das leis de proteção de dados nos Estados Unidos, integrando as visões de autores renomados como Danilo Doneda, Bruno Bioni e outras perspectivas contemporâneas. O objetivo é identificar semelhanças, diferenças e impactos dessas legislações, considerando a evolução recente do campo da proteção de dados pessoais. São examinados os princípios fundamentais, as bases legais de tratamento, as responsabilidades das entidades que lidam com dados e os direitos dos titulares, bem como os mecanismos de fiscalização e as consequências regulatórias para empresas e instituições em um cenário globalizado.

Palavras-chave: Abordagem. Consentimento. Dados pessoais. Direitos dos titulares. LGPD. Proteção de dados. Responsabilidade das entidades.onciliação. Resolução de conflitos. Pacificação social. Diálogo.

ABSTRACT: This paper proposes a comprehensive and updated analysis of Brazil's General Data Protection Law (LGPD) and data protection laws in the United States, integrating views from renowned authors such as Danilo Doneda, Bruno Bioni and other contemporary perspectives. The objective is to identify similarities, differences and impacts of these legislations, considering recent developments in the field of personal data protection. It examines fundamental principles, legal bases for processing, the responsibilities of entities handling data and the rights of data subjects, as well as supervisory mechanisms and regulatory consequences for companies and institutions in a globalized environment.

Keywords: Approach. Consent. Data protection. Data subject rights. LGPD. Personal data. Entity responsibility.

[1]Bacharel em Comunicação Social. Bacharel em Direito. Pós- graduado em Direito Constitucional. Mestre em Ciências jurídicas, com ênfase em Direito Internacional. Doutorando de Direito pela São Luís University, Orcid: https://orcid.org/0009-0001-0310-9488 .
[2]Bacharela em Direito. Pós-graduada em Direito Penal; Pós-graduada em Direito Constitucional; Mestre em Ciências jurídicas, com ênfase em Direito Internacional. Doutoranda de Direito pela São Luís University. Orcid: https://orcid.org/0009-0005-1585-5399.
[3]Bacharela em Direito. Pós-graduada em Perícias de Avaliação Patrimonial de Bens e Direitos; Pós-graduada em Direito Constitucional; Mestre em Ciências jurídicas, com ênfase em Direito Internacional. Doutoranda de Direito pela São Luís University. Orcid: https://orcid.org/0009-0003-8715-3754.
[4]Bacharel em Direito; Pós-graduado em Direito Penal; Pós-graduado em Direito das Relações Sociais com área de concentração em Direito Processual; Mestre em Ciências Jurídicas, com ênfase em Direito Internacional; Doutorando de Direito pela São Luís University. Orcid: https://orcid.org/0009-0008-2072-8126.
[5]Bacharel em Direito. Pós-graduado em Direito Constitucional, Administrativo e Tributário. Mestre em Direito Agrário. Doutorando de Direito pala São Luís University. Orcid: http://orcid.org/0009-0005-3677-1071.

1 INTRODUÇÃO

O crescente avanço tecnológico e a ubiquidade da internet ressaltam a necessidade de proteger os dados pessoais dos indivíduos. Plataformas digitais, serviços em nuvem, sistemas de inteligência artificial e práticas de Big Data intensificam a coleta, o armazenamento e o compartilhamento de informações, tornando a proteção de dados um dos temas centrais do direito contemporâneo. Nesse contexto, a Lei Geral de Proteção de Dados (LGPD), no Brasil, e o mosaico de legislações setoriais existentes nos Estados Unidos emergem como respostas normativas a demandas sociais, econômicas e políticas cada vez mais complexas.

O presente estudo tem como objetivo oferecer uma análise comparativa entre a LGPD e as normas de proteção de dados norte-americanas, evidenciando convergências e divergências em relação a princípios, estrutura regulatória, proteção dos titulares e responsabilidades das entidades que tratam dados. Para enriquecer essa análise, são consideradas as contribuições de Danilo Doneda e Bruno Bioni, cujos estudos situam a proteção de dados no âmbito dos direitos fundamentais, da autodeterminação informativa e da governança responsável da informação.

A pesquisa justifica-se pela importância de compreender como diferentes modelos jurídicos respondem a desafios semelhantes, em especial em um cenário em que fluxos internacionais de dados se intensificam e exigem padrões mínimos de convergência. Ao analisar comparativamente a legislação brasileira e a realidade norte-americana, busca-se contribuir para o debate sobre a consolidação de uma cultura de proteção de dados, voltada tanto à tutela dos indivíduos quanto à segurança jurídica das organizações.

2 PROTEÇÃO DE DADOS PESSOAIS E OBRIGAÇÕES PARA ENTIDADES

A proteção de dados pessoais e as obrigações das entidades que tratam essas informações passa a configurarm eixo central da legislação contemporânea sobre privacidade. Na LGPD, os dados pessoais são definidos como informações relacionadas a pessoa natural identificada ou identificável, e o tratamento deve observar princípios como finalidade, adequação, necessidade, transparência, segurança, prevenção e responsabilização. Doneda destaca que a proteção de dados não se limita a um aspecto meramente informacional, mas se conecta diretamente à dignidade da pessoa humana e à proteção contra formas de vigilância e discriminação.

Autores como Doneda e Bioni enfatizam a relevância do consentimento informado como uma das bases legais para o tratamento de dados. Esse consentimento deve ser livre, informado, inequívoco e específico, permitindo que o titular compreenda de maneira clara as

finalidades do tratamento e os riscos envolvidos. Ao mesmo tempo, Bioni adverte que a centralidade exclusiva do consentimento é insuficiente em contextos complexos, motivo pelo qual a LGPD adota um conjunto diversificado de bases legais, como o cumprimento de obrigação legal, a execução de contratos, o exercício regular de direitos e o legítimo interesse do controlador.

A responsabilidade das entidades que tratam dados pessoais também é sublinhada de forma intensa pela doutrina. A LGPD exige a adoção de medidas técnicas e organizacionais aptas a proteger os dados contra acessos não autorizados, vazamentos, destruição acidental ou ilícita e qualquer forma de uso inadequado. Isso inclui políticas de segurança, controles de acesso, registro de operações de tratamento, programas de governança em privacidade e capacitação contínua de equipes. A lógica da responsabilização (accountability) perpassa toda a legislação, impondo às organizações não apenas o dever de cumprir a norma, mas de evidenciar, de forma transparente, como atingem a conformidade.

Nos Estados Unidos, o tratamento de dados pessoais não é regido por uma lei geral, mas por um conjunto de legislações setoriais. Leis como a Health Insurance Portability and Accountability Act (HIPAA), no setor de saúde, o Gramm-Leach-Bliley Act (GLBA), no setor financeiro, e a Children's Online Privacy Protection Act (COPPA), para dados de crianças, estabelecem obrigações específicas, enquanto normas estaduais como a California Consumer Privacy Act (CCPA) aproximam-se de modelos mais abrangentes. Ainda assim, a ausência de uma lei federal unificada gera lacunas e desafios na consolidação de um padrão uniforme de responsabilidade.

3 ESCOPO REGULATÓRIO E ABORDAGEM LEGAL

A LGPD caracteriza-se como uma lei de escopo geral, aplicável a qualquer operação de tratamento de dados pessoais realizada no território nacional ou que tenha por objetivo a oferta ou fornecimento de bens ou serviços a indivíduos localizados no Brasil. Seu enfoque recai sobre a proteção de direitos fundamentais, como privacidade, honra, imagem e liberdade de expressão, estruturando um regime jurídico coerente, independente do setor econômico em que se dá o tratamento.

Nos Estados Unidos, a abordagem é fragmentada e setorial. Em vez de um único diploma normativo de proteção de dados pessoais, há um conjunto de leis federais e estaduais que regulam aspectos específicos do tratamento de informações. A CCPA, implementada na

Califórnia, tornou-se um marco ao conferir aos consumidores direitos como acesso às informações coletadas, possibilidade de exclusão de dados e opção de impedir a venda de suas informações pessoais. No entanto, sua aplicação é territorial e não substitui a ausência de uma lei geral nacional.

A doutrina contemporânea observa que essa multiplicidade de normas cria uma espécie de mosaico regulatório, no qual empresas que atuam em vários estados precisam manejar regimes distintos, aumentando custos de conformidade e complexidade operacional. Em contraste, a LGPD, ao adotar um modelo unificado, facilita a criação de políticas internas de proteção de dados uniformes e confere maior previsibilidade jurídica, embora também imponha desafios de adaptação às organizações.

4 DIREITOS DOS TITULARES DE DADOS

Os direitos dos titulares de dados pessoais constituem o eixo normativo central da Lei Geral de Proteção de Dados Pessoais (LGPD), refletindo a opção legislativa por um modelo de proteção orientado à centralidade do indivíduo e ao controle social sobre o uso da informação. Ao consagrar um conjunto amplo de direitos, a LGPD busca corrigir as assimetrias estruturais existentes nas relações entre titulares e agentes de tratamento, especialmente em um contexto marcado pela crescente concentração informacional, pela automatização de decisões e pela opacidade dos fluxos de dados no ambiente digital.

A titularidade dos dados pessoais, embora não implique direito de propriedade no sentido clássico, confere ao indivíduo prerrogativas jurídicas que lhe permitem influenciar de maneira significativa as decisões relativas ao tratamento de suas informações. Danilo Doneda ressalta que a proteção de dados deve ser compreendida como desdobramento contemporâneo da tutela da personalidade, vinculando-se diretamente à dignidade da pessoa humana e à liberdade individual. Nesse sentido, os direitos dos titulares operam como instrumentos de autodeterminação informativa, assegurando ao sujeito a possibilidade de participar ativamente das escolhas que afetam sua esfera informacional.

Entre os direitos expressamente previstos pela LGPD, destaca-se inicialmente o direito de confirmação da existência de tratamento e de acesso aos dados pessoais, que permite ao titular conhecer se suas informações estão sendo tratadas, por quem e para quais finalidades. Tal direito constitui pressuposto para o exercício dos demais, pois somente a partir do conhecimento sobre o tratamento é possível avaliar sua licitude e adequação. A esse respeito,

Bruno Bioni observa que a transparência informacional representa condição indispensável para a efetividade da proteção de dados, uma vez que reduz a assimetria de informações entre titulares e controladores.

A LGPD assegura, ainda, o direito à correção de dados incompletos, inexatos ou desatualizados, bem como à anonimização, ao bloqueio ou à eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a legislação. Esses direitos expressam a preocupação do legislador com a qualidade dos dados e com a limitação do tratamento ao estritamente necessário para o atendimento de finalidades legítimas. A eliminação e a anonimização, em particular, revelam-se instrumentos relevantes para a redução de riscos associados ao armazenamento prolongado de informações pessoais, mitigando potenciais danos decorrentes de vazamentos ou usos indevidos.

Outro direito de especial relevância é a portabilidade dos dados a outro fornecedor de serviço ou produto, observados os segredos comercial e industrial. A portabilidade visa promover a concorrência e evitar a retenção artificial de titulares por grandes plataformas digitais, conferindo maior liberdade de escolha aos indivíduos. Embora sua implementação envolva desafios técnicos e regulatórios, a doutrina reconhece que esse direito pode contribuir para a construção de mercados mais justos e transparentes, desde que acompanhado de padrões interoperáveis e de garantias de segurança da informação.

O direito à informação clara e adequada acerca do uso compartilhado de dados pessoais com entidades públicas e privadas também ocupa posição de destaque na LGPD. Esse direito reforça o dever de transparência dos controladores e permite ao titular avaliar os riscos associados à circulação de seus dados em cadeias complexas de tratamento. Além disso, a possibilidade de revogação do consentimento, a qualquer tempo, reafirma o caráter dinâmico da vontade do titular, impedindo que autorizações concedidas em determinado contexto sejam utilizadas de forma indefinida ou desvinculada das expectativas legítimas do indivíduo.

A doutrina enfatiza que a efetividade desses direitos depende de sua operacionalização concreta pelas organizações. Não basta o reconhecimento formal das prerrogativas do titular; é necessário que os agentes de tratamento disponham de estruturas organizacionais, técnicas e procedimentais que viabilizem o exercício desses direitos de maneira célere, acessível e não discriminatória. Canais de atendimento eficientes, políticas de privacidade redigidas em linguagem clara e sistemas capazes de localizar, corrigir ou eliminar dados de forma segura são elementos indispensáveis para a concretização da proteção conferida pela LGPD.

No sistema norte-americano, a proteção dos direitos dos titulares de dados ocorre de forma fragmentada e desigual. Leis estaduais como a California Consumer Privacy Act (CCPA) e a California Privacy Rights Act (CPRA) reconhecem direitos de acesso, correção, exclusão e oposição à venda de dados pessoais, aproximando-se, em certa medida, do modelo europeu e brasileiro. Contudo, a ausência de uma lei federal geral implica que tais direitos não sejam assegurados de maneira uniforme em todo o território dos Estados Unidos, gerando disparidades significativas na tutela conferida aos cidadãos.

Sob uma perspectiva comparada, a LGPD destaca-se por oferecer um regime sistemático e coerente de direitos dos titulares, integrando-os a um conjunto mais amplo de deveres e mecanismos de responsabilização. Ao colocar o titular no centro da regulação, a legislação brasileira contribui para a consolidação de uma cultura jurídica orientada à proteção da pessoa humana no ambiente digital, reforçando a ideia de que o tratamento de dados pessoais deve servir a finalidades legítimas, proporcionais e socialmente justificáveis.

5 FISCALIZAÇÃO E APLICAÇÃO DE PENALIDADES

A efetividade dos regimes contemporâneos de proteção de dados pessoais está diretamente relacionada à existência de estruturas institucionais capazes de fiscalizar o cumprimento das normas e de aplicar sanções proporcionais, adequadas e juridicamente fundamentadas. A Lei Geral de Proteção de Dados Pessoais (LGPD), ao instituir um sistema próprio de responsabilização, buscou superar modelos meramente declaratórios, conferindo densidade normativa às garantias previstas em lei por meio da atuação de uma autoridade especializada.

No contexto brasileiro, a Autoridade Nacional de Proteção de Dados (ANPD) ocupa posição central nesse arranjo institucional. Compete à ANPD zelar pela proteção dos dados pessoais, fiscalizar e orientar os agentes de tratamento, editar normas complementares, promover ações educativas e aplicar sanções administrativas. A criação da autoridade representa avanço institucional relevante, pois permite a uniformização interpretativa da LGPD, a indução de boas práticas e a consolidação de uma política nacional de proteção de dados, contribuindo para a redução de incertezas jurídicas e para o fortalecimento da segurança regulatória.

A atuação da ANPD não se restringe à repressão de infrações já consumadas. A autoridade exerce funções preventivas e pedagógicas, estimulando a adoção de mecanismos de governança em privacidade e de gestão de riscos associados ao tratamento de dados pessoais. A

edição de guias orientativos, regulamentos setoriais e recomendações técnicas evidencia que o modelo brasileiro privilegia uma lógica regulatória progressiva, na qual a sanção administrativa é concebida como instrumento de última ratio, a ser utilizado quando frustradas as estratégias de orientação e conformidade voluntária. Essa abordagem dialoga com a perspectiva defendida por Bruno Bioni, segundo a qual a responsabilização deve funcionar como vetor de transformação das práticas organizacionais, promovendo padrões éticos e responsáveis no uso da informação.

As sanções administrativas previstas na LGPD abrangem advertência, multa simples ou diária, publicização da infração, bloqueio e eliminação dos dados pessoais relacionados à irregularidade, bem como a suspensão parcial ou total do exercício das atividades de tratamento. O regulamento de dosimetria editado pela ANPD estabelece critérios objetivos para a aplicação dessas penalidades, considerando elementos como a natureza e a gravidade da infração, os danos causados aos titulares, a vantagem auferida pelo infrator, a reincidência e o grau de cooperação com a autoridade reguladora. Busca-se, assim, assegurar proporcionalidade e razoabilidade na resposta estatal, evitando tanto a ineficácia das sanções quanto o excesso punitivo.

A lógica sancionatória da LGPD encontra-se intrinsecamente vinculada ao princípio da responsabilização e prestação de contas (accountability). Conforme destaca Danilo Doneda, a proteção de dados pessoais exige que os agentes de tratamento sejam capazes de demonstrar, de forma contínua, transparente e documentada, a conformidade de suas práticas com a legislação. Programas de governança em privacidade, relatórios de impacto à proteção de dados pessoais e políticas internas estruturadas constituem instrumentos centrais nesse processo, funcionando simultaneamente como mecanismos de prevenção de riscos e como elementos atenuantes na eventual aplicação de sanções.

Nos Estados Unidos, a fiscalização do tratamento de dados pessoais apresenta configuração significativamente distinta. A inexistência de uma autoridade nacional única e de um regime geral de proteção de dados resulta em uma estrutura descentralizada, na qual diferentes órgãos exercem competências fiscalizatórias conforme o setor regulado. A Federal Trade Commission (FTC) desempenha papel de destaque ao atuar em casos de práticas comerciais desleais ou enganosas relacionadas à privacidade e à segurança da informação, utilizando instrumentos típicos do direito do consumidor para coibir condutas abusivas.

Além da FTC, agências setoriais específicas são responsáveis pela fiscalização e aplicação de sanções em áreas como saúde, finanças e telecomunicações, a exemplo do

Department of Health and Human Services (HHS) no âmbito da Health Insurance Portability and Accountability Act (HIPAA). Essa fragmentação institucional, embora permita respostas especializadas a determinados contextos, dificulta a construção de uma política nacional coesa de proteção de dados pessoais. A ausência de critérios uniformes de responsabilização e de coordenação regulatória gera assimetrias na tutela conferida aos titulares e respostas desiguais a incidentes de segurança e violações de privacidade.

Sob a perspectiva comparada, o modelo brasileiro apresenta maior potencial de coerência sistêmica ao concentrar a fiscalização em uma autoridade especializada e ao estruturar um regime sancionatório transparente, orientado por critérios objetivos e por uma lógica de indução à conformidade. A centralização das competências na ANPD favorece a consolidação de entendimentos estáveis e a difusão de padrões consistentes de governança em privacidade. Em contraste, o modelo norte-americano, apesar de avanços relevantes em iniciativas estaduais e setoriais, permanece marcado por uma arquitetura fragmentada, que limita a efetividade da proteção de dados diante dos desafios impostos pela economia digital e pelos fluxos transnacionais de informações pessoais.

6 APLICABILIDADE EXTRATERRITORIAL E IMPACTO EMPRESARIAL

A LGPD, em sintonia com o Regulamento Geral de Proteção de Dados europeu (GDPR), adota cláusulas de aplicabilidade extraterritorial. Isso significa que empresas estrangeiras que tratam dados de indivíduos localizados no Brasil, oferecendo-lhes bens ou serviços, também estão sujeitas à legislação brasileira. Essa opção legislativa procura evitar que organizações se esquivem da responsabilidade por meio da localização de seus servidores em outros países.

A extraterritorialidade amplia o alcance da proteção de dados, mas, ao mesmo tempo, impõe às empresas o desafio de conciliar múltiplas legislações nacionais e regionais. Autores contemporâneos observam que, para muitas organizações, o cumprimento simultâneo de GDPR, LGPD, CCPA e outras normas locais exige sofisticados programas de conformidade, revisões contratuais e investimentos em tecnologia e governança. Por outro lado, a adoção de altos padrões de proteção pode converter-se em vantagem competitiva, reforçando a confiança de consumidores e parceiros comerciais.

Nos Estados Unidos, a extraterritorialidade é tratada de forma mais limitada e pontual, vinculada às especificidades de cada legislação. A CCPA, por exemplo, aplica-se a determinadas

empresas que coletam informações de residentes na Califórnia, ainda que sediadas fora do estado. Todavia, a ausência de um marco federal impede a adoção de uma política extraterritorial uniforme em âmbito nacional.

7 CONCLUSÃO

A comparação entre a legislação brasileira de proteção de dados, representada pela LGPD, e o sistema norte-americano, composto por normas setoriais e estaduais, evidencia duas matrizes distintas de regulação da privacidade e da segurança informacional. O modelo brasileiro, inspirado no paradigma europeu, adota uma abordagem unificada e principiológica, com forte ênfase nos direitos dos titulares, na responsabilização das entidades e na atuação de autoridade especializada. Já o cenário dos Estados Unidos mantém-se fragmentado, com leis específicas para determinados setores e iniciativas estaduais que avançam em direção a maior tutela, sem, contudo, constituir um regime geral nacional.

As contribuições de Danilo Doneda e Bruno Bioni demonstram que a proteção de dados não deve ser compreendida apenas como instrumento de regulação econômica, mas como dimensão essencial dos direitos fundamentais. Ao enfatizarem temas como autodeterminação informativa, responsabilidade, transparência e governança, esses autores apontam para a necessidade de políticas públicas que articulem regulação, educação digital e mecanismos institucionais eficazes.

No contexto global, a tendência é de crescente convergência entre modelos regulatórios, seja por influência de legislações de referência — como o GDPR e a própria LGPD —, seja pela necessidade de estabelecer condições mínimas de segurança jurídica em fluxos transnacionais de dados. Ainda assim, persistem desafios relacionados à implementação efetiva das normas, à estruturação de autoridades reguladoras, ao desenvolvimento de culturas organizacionais comprometidas com a privacidade e à superação de assimetrias informacionais entre indivíduos e grandes corporações.

Em síntese, a análise empreendida indica que a LGPD representa avanço significativo para o ordenamento jurídico brasileiro, alinhando-o a padrões internacionais de proteção de dados, ao passo que o modelo norte-americano, embora disponha de importantes instrumentos legais, ainda carece de maior unidade e coerência sistêmica. A consolidação de um ambiente digital mais seguro, ético e transparente depende, em última instância, da articulação entre leis

eficazes, instituições fortes e uma sociedade consciente de seus direitos e responsabilidades no tratamento de dados pessoais.

REFERÊNCIAS

BIONI, B. Dados pessoais: o novo petróleo. Belo Horizonte: Letramento, 2018.

BIONI, B. Proteção de dados pessoais: a função e os limites do consentimento. São Paulo: Thomson Reuters Brasil, 2021.

BIONI, B. Lei Geral de Proteção de Dados Pessoais comentada. Salvador: Juspodivm, 2023.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Brasília, 2023.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Guia Orientativo para Comunicação de Incidentes de Segurança. Brasília, 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF.

CALIFORNIA. California Privacy Rights Act (CPRA). 2020, com vigência plena a partir de 2023.

DONEDA, D. Privacidade, proteção de dados e defesa do consumidor. São Paulo: Revista dos Tribunais, 2020.

DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

DONEDA, D. Proteção de dados pessoais: comentários à Lei nº 13.709/2018. Rio de Janeiro: Forense, 2019.

EUROPEAN UNION. General Data Protection Regulation (GDPR). Regulation (EU) 2016/679.

MENDES, L.S. Privacidade, proteção de dados e defesa do consumidor no Brasil. São Paulo: Revista dos Tribunais, 2014.

UNITED STATES. Federal Trade Commission. Privacy and Data Security Update. Washington, 2024.

ZANATTA, R.A.F. Proteção de dados pessoais, concorrência e regulação. São Paulo: Almedina, 2022.