A proteção de dados sensíveis sob a lei geral de proteção de dados lei 13.709/18 (LGPD): desafios e perspectivas

The protection of sensitive data under the general data **protection** *law 13.709/18 (LGPD): challenges and perspectives*

Rafael Kouji Kina Berengue, Curso de direito, Centro universitário Integrado, Brasil, Rafael.berengue@gmail.com.

Andreia Aparecida de Souza, Professora Orientadora, Curso de direito, Centro universitário Integrado, Brasil, andreia.souza@grupointegrado.br.

Resumo: Este artigo analisa o tratamento conferido aos dados pessoais sensíveis pela Lei Geral de Proteção de Dados (LGPD) brasileira, avaliando sua eficácia na proteção dos direitos fundamentais dos cidadãos e os desafios enfrentados por organizações e indivíduos na implementação e cumprimento das disposições legais. A pesquisa examina o conceito de dados sensíveis, analisa os princípios e disposições específicas da LGPD, investiga os impactos práticos da lei e avalia a efetividade da tutela dos direitos fundamentais relacionados à proteção de dados sensíveis. Utilizando o método dedutivo e a abordagem de revisão de literatura, o estudo faz uma análise crítica da legislação, jurisprudência e doutrina, com o intuito de contribuir para o aprimoramento da proteção de dados no Brasil, considerando as tendências internacionais e os desafios futuros neste campo.

Palavras-chave: LGPD. Dados sensíveis. Proteção de dados. Direitos fundamentais. Privacidade.

Abstract: This article analyzes the treatment granted to sensitive personal data by the Brazilian General Data Protection Law (LGPD), evaluating its effectiveness in protecting citizens' fundamental rights and the challenges faced by organizations and individuals in implementing and complying with legal provisions. The research examines the concept of sensitive data, analyzes the principles and specific provisions of the LGPD, investigates the practical impacts of the law and evaluates the effectiveness of the protection of fundamental rights related to the protection of sensitive data. Using the deductive method and the literature review approach, the study makes a critical analysis of legislation, jurisprudence and doctrine, with the aim of contributing to the improvement of data protection in Brazil, considering international trends and future challenges in this field.

Keywords: LGPD. Sensitive data. Data protection. Fundamental rights. Privacy.

INTRODUÇÃO

O Direito, como mecanismo de regulação de conduta, deve reverberar a realidade da sociedade. Neste sentido, o direito digital se apresenta como a evolução necessária para reger as relações jurídicas em ambientes virtuais. Concernente a isto, nasce a preocupação com a proteção dos dados pessoais, que possui sua origem na privacidade.

Atualmente, as questões que envolvem a égide aos direitos da personalidade, sobretudo a garantia à privacidade e intimidade, trazem em discussão a importância de se proteger os dados pessoais, como meio de eficácia dos direitos humanos, fundamentalmente constitucionais.

Os desdobramentos e repercussões que permeiam a proteção dos dados pessoais são mundialmente discutidos. Temos como exemplo de efetivo tratamento e regulação, no direito comparado, a Comunidade Europeia, que possui um Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês) capaz de conferir aos titulares dos dados um maior controle e às autoridades um mecanismo sólido e unificado para aplicação.

No Brasil, a matéria ganha destaque jurídico-legislativo com a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD). A Lei foi sancionada no ano de 2018 e após o seu período de vacatio legis, permeado de algumas incertezas, entrou em vigor no ano de 2020.

A lei brasileira se funda na proteção de direitos fundamentais, instituindo regras para o tratamento dos dados pessoais, que deverão ser observadas por instituições públicas e privadas, objetivando determinar o comportamento das instituições no tratamento de dados pessoais dos indivíduos, isto é, o tratamento sobre dados identificados ou identificáveis de pessoas naturais, estabelecendo parâmetros de coleta, armazenamento, processamento e extinção destas informações.

Neste contexto, a proteção de dados sensíveis emerge como um tema de particular importância.

A LGPD define dados sensíveis como aqueles sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Estes dados requerem um nível de proteção ainda mais elevado devido ao seu potencial de causar discriminação ou prejuízos significativos aos indivíduos, caso sejam indevidamente expostos ou utilizados.

A implementação da LGPD tem gerado impactos significativos nas práticas de tratamento de dados por parte de empresas e organizações brasileiras, especialmente no que diz respeito aos dados sensíveis.

Estas mudanças são profundas e abrangentes, envolvendo uma revisão completa das políticas de privacidade, a implementação de medidas técnicas e organizacionais de segurança reforçadas, e o desenvolvimento de processos para obtenção e gestão do consentimento específico.

A relevância dessa proteção é evidenciada por diversos casos de violações de dados sensíveis ocorridos globalmente.

Em 2016, por exemplo, a Red Cross Blood Service na Austrália sofreu um vazamento de dados que expôs informações de 550.000 doadores de sangue, incluindo detalhes sensíveis sobre comportamentos sexuais considerados de risco.

Em 2017, no Canadá, a empresa Standard Innovation enfrentou uma ação coletiva após descobrir-se que seu produto, um vibrador conectado, coletava e transmitia dados sensíveis sobre o uso do dispositivo sem o consentimento adequado dos usuários.

Mais recentemente, em 2018, o caso do Facebook-Cambridge Analytica trouxe à tona questões cruciais sobre a proteção de dados sensíveis em plataformas de redes sociais.

Neste incidente, dados de milhões de usuários do Facebook foram coletados sem consentimento adequado e utilizados para fins de direcionamento político, levantando sérias preocupações sobre privacidade, manipulação de opinião pública e integridade democrática.

Estes casos ilustram a complexidade e a urgência da proteção de dados sensíveis na era digital.

A implementação de legislações como a LGPD torna-se, portanto, crucial para estabelecer diretrizes claras e garantir a proteção efetiva desses dados.

No entanto, a eficácia dessas leis depende não apenas de sua formulação, mas também de sua aplicação prática e da conscientização tanto de organizações quanto de indivíduos sobre a importância da proteção de dados sensíveis.

Este estudo tem como objetivo principal analisar criticamente o tratamento conferido aos dados pessoais sensíveis pela LGPD, avaliando sua eficácia na proteção dos direitos fundamentais dos cidadãos brasileiros e os desafios enfrentados por organizações e indivíduos na implementação e cumprimento das disposições legais.

Através de uma análise abrangente da legislação, jurisprudência e casos práticos, busca-se contribuir para o aprimoramento da proteção de dados sensíveis no Brasil, considerando as tendências internacionais e os desafios futuros neste campo em constante evolução.

MÉTODO

Este estudo adota uma abordagem de revisão de literatura, com base no método dedutivo, e utiliza pesquisa bibliográfica e documental para realizar uma análise crítica sobre a proteção de dados sensíveis no âmbito da Lei Geral de Proteção de Dados (LGPD) no Brasil.

O método dedutivo permite que a investigação se inicie a partir das disposições legais, doutrinárias e jurisprudenciais gerais, analisando a proteção de direitos fundamentais relacionados à privacidade e aos dados pessoais e, a partir desses fundamentos, deduza conclusões sobre a eficácia e os desafios específicos da legislação na proteção de dados sensíveis.

A revisão bibliográfica incluiu a análise de livros, artigos acadêmicos e publicações especializadas sobre a proteção de dados pessoais, com foco na LGPD e na tutela de dados sensíveis.

Entre os doutrinadores consultados, destaca-se Danilo Doneda, um dos principais estudiosos brasileiros na área de privacidade e proteção de dados. Em suas obras, Doneda destaca a importância de um tratamento jurídico adequado

aos dados sensíveis, considerando-os essenciais para a proteção dos direitos da personalidade no ambiente digital.

Suas contribuições foram fundamentais para a formulação da LGPD, especialmente na definição e proteção dos dados sensíveis.

A análise documental envolveu o exame detalhado da LGPD, legislações correlatas e jurisprudência relevante, objetivando compreender como essas normativas são aplicadas e quais desafios surgem na implementação da proteção de dados sensíveis.

A partir desse estudo das normas e da prática, deduz-se o grau de efetividade e as dificuldades enfrentadas por instituições públicas e privadas no cumprimento da legislação.

A escolha pelo método dedutivo é justificada pela natureza exploratória do tema, que exige uma compreensão detalhada da doutrina e legislação para, a partir desses conceitos gerais, deduzir as particularidades e impactos da proteção de dados sensíveis na sociedade contemporânea.

RESULTADOS E DISCUSSÃO

1 CONTEXTUALIZAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709 de 14 de agosto de 2018, representa um marco significativo na legislação brasileira sobre proteção de dados pessoais.

Embora o Brasil já contasse com dispositivos constitucionais e leis esparsas que abordavam aspectos da privacidade e proteção de dados, como o Código de Defesa do Consumidor e o Marco Civil da Internet, a LGPD é o primeiro instrumento legal abrangente e específico sobre o tema no país.

A lei foi fortemente inspirada em modelos internacionais, notadamente o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia (BIONI; MENDES, 2019), e busca alinhar-se às diretrizes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), refletindo o interesse do Brasil em integrar esta organização como membro.

O surgimento da LGPD é uma resposta direta aos desafios impostos pelo rápido desenvolvimento tecnológico e pela globalização, que criaram um cenário de negócios internacionais praticamente sem fronteiras.

Neste contexto, a necessidade de regulamentação específica para proteger os dados pessoais tornou-se premente.

A LGPD busca estabelecer um equilíbrio entre a proteção dos direitos humanos fundamentais e a viabilização das transações comerciais que dependem do fluxo de dados pessoais.

O objetivo principal da LGPD é proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural. Seu escopo é amplo, abrangendo o tratamento de dados pessoais por pessoas físicas e jurídicas, de direito público ou privado, com finalidade econômica.

É importante ressaltar que a lei se aplica ao tratamento de dados tanto em meios digitais quanto offline, demonstrando sua abrangência e adaptabilidade aos diversos contextos de coleta e processamento de informações pessoais.

Estruturada em dez capítulos, a LGPD aborda diversos aspectos da proteção de dados, desde princípios e direitos do titular até sanções administrativas. A lei estabelece uma distinção clara entre dados pessoais "comuns" e dados sensíveis, enquanto os primeiros já gozam de proteção significativa, estes últimos recebem um nível mais elevado de proteção (MULHOLLAND, 2020).

Os princípios fundamentais da lei incluem a boa-fé, a transparência e a liberdade, visando estabelecer um modelo de conduta adequado para garantir a observância dos direitos humanos no contexto do tratamento de dados pessoais.

A jurisprudência brasileira já começou a se manifestar sobre casos envolvendo o tratamento de dados sensíveis. Por exemplo, o Superior Tribunal de Justiça, no julgamento do Recurso Especial nº 1.758.799/MG, abordou a questão do tratamento de dados de saúde por planos de saúde, enfatizando a necessidade de respeito à privacidade e ao sigilo médico (BRASIL, 2019).

A implementação da LGPD tem provocado uma movimentação significativa em diversos setores da sociedade brasileira, impondo a necessidade de adaptação tanto para instituições públicas quanto privadas no que tange às operações que envolvem o tratamento de dados pessoais.

A lei prevê a criação da Autoridade Nacional de Proteção de Dados (ANPD), um órgão responsável por zelar pela implementação e fiscalização da lei.

É importante notar que a LGPD estabelece algumas exceções à sua aplicação.

Por exemplo, o tratamento de dados realizado por pessoa natural para fins exclusivamente particulares e não econômicos não está sujeito às regulações da lei. Essas exceções visam equilibrar a proteção dos dados pessoais com as necessidades práticas da vida cotidiana e de certas atividades específicas.

Em suma, a LGPD representa um avanço significativo na proteção dos dados pessoais no Brasil, alinhando o país com as melhores práticas internacionais e estabelecendo um framework robusto para o tratamento ético e responsável das informações pessoais dos cidadãos. Sua implementação continua a ser um processo em evolução, com desafios e adaptações sendo enfrentados por organizações e indivíduos à medida que buscam cumprir com as novas exigências legais.

2 DEFINIÇÃO E CLASSIFICAÇÃO DOS DADOS PESSOAIS.

A LGPD em seu artigo 5°, inciso I, define dado pessoal como "informação relacionada a pessoa natural identificada ou identificável" (BRASIL,2018).

Esta definição abrangente engloba uma ampla gama de informações que podem, direta ou indiretamente, identificar um indivíduo. A classificação dos dados pessoais em categorias específicas, como dados sensíveis, é fundamental para determinar o nível de proteção necessário.

Os dados sensíveis são uma categoria especial de dados pessoais que, devido à sua natureza, requerem proteção adicional.

A LGPD define em seu artigo 5°, inciso II, dados sensíveis como aqueles sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2018).

Na visão de Tepedino (2020, p. 45) a relevância jurídica dos dados sensíveis está intrinsecamente ligada ao seu potencial de causar discriminação ou prejudicar direitos fundamentais dos indivíduos:

> Os dados sensíveis, por sua natureza, estão intimamente ligados à personalidade do indivíduo e, se mal utilizados, podem gerar situações de discriminação e violação de direitos fundamentais, como a dignidade da pessoa humana, a igualdade e a privacidade.

A proteção de dados pessoais, especialmente os sensíveis, está diretamente relacionada à tutela de diversos direitos fundamentais consagrados na Constituição Federal (BRASIL, 1988), como o direito à privacidade, à intimidade, à honra e à imagem. A LGPD reconhece explicitamente esta conexão, estabelecendo como um de seus fundamentos o respeito à privacidade e à autodeterminação informativa.

Esta proteção se alinha com a concepção de direitos fundamentais presente na Constituição Federal de 1988, também conhecida como "Constituição Cidadã", a Constituição de 1988 preconiza o constitucionalismo democrático, colocando a soberania do povo e o respeito aos direitos fundamentais como critérios norteadores.

O artigo 5º, inciso X, da Constituição Federal (BRASIL, 1988), estabelece explicitamente a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos

> estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> [...]
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
>
> [...]

A tutela constitucional desses direitos fundamentais se estende à proteção de dados pessoais na era digital.

Como observa Anderson Schreiber (2014, p. 32), com relação ao direito de privacidade:

> O direito à privacidade hoje é mais amplo que o simples direito à intimidade. Não se limita ao direito de cada um de ser 'deixado só' ou de impedir a intromissão alheia na sua vida íntima e particular. Transcende essa esfera doméstica para alcançar qualquer ambiente onde circulam dados pessoais do seu titular, aí incluídos suas características físicas, código genético, estado de saúde, crença religiosa e qualquer outra informação pertinente à pessoa.

Desta forma, a proteção de dados pessoais, especialmente os sensíveis, se configura como uma extensão moderna e necessária dos direitos fundamentais à privacidade e à intimidade, adaptando-se aos desafios impostos pela sociedade da informação e pela evolução tecnológica.

A LGPD, ao regular o tratamento de dados pessoais, atua como um instrumento de concretização desses direitos fundamentais no contexto digital, reforçando a tutela constitucional da pessoa humana frente aos riscos inerentes ao fluxo massivo de informações pessoais na era da internet.

3 PRINCÍPIOS E DISPOSIÇÕES DA LGPD SOBRE DADOS SENSÍVEIS

A Lei Geral de Proteção de Dados Pessoais (LGPD - Lei 13.709/18) estabelece um marco regulatório abrangente para o tratamento de dados pessoais no Brasil, com implicações significativas para o manejo de dados sensíveis.

A lei reconhece a finalidade da tutela desses dados para a proteção de direitos fundamentais, como liberdade de expressão, privacidade, honra, imagem e autodeterminação informativa.

Além disso, a LGPD enfatiza a promoção de Direitos Humanos Fundamentais como justificativa para a proteção de dados pessoais.

A LGPD possui um real escopo de manual sobre tratamento de dados pessoais, não setorizando finalidades, mas regulando de forma abrangente as diversas implicações que o manuseio de dados pessoais de terceiros requer.

O espírito da lei é a proteção de direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade de pessoas naturais. Sua tutela destina-se a salvaguardar os dados de pessoas físicas, portanto, dados pessoais, não incluindo os dados de pessoas jurídicas em sua finalidade.

O escopo da LGPD é amplo, abrangendo uma vasta gama de operações de tratamento de dados, incluindo coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão e extração, com base no artigo 3° da LGPD (BRASIL, 2018):

> Art. 5º Para os fins desta Lei, considera-se:
>
> [...]
>
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
>
> [...]

A lei se aplica tanto ao ambiente digital quanto fora dele, abrangendo o tratamento de dados online e offline.

No entanto, a lei prevê exceções importantes, como o tratamento por pessoas naturais para fins particulares e não econômicos, o tratamento para fins exclusivamente jornalísticos, artísticos ou acadêmicos, e o tratamento para fins de segurança pública, defesa nacional ou investigação criminal, entre outros.

Além disso, a lei não se aplica aos casos em que os dados possuam origem fora do território brasileiro, se por acaso não houver compartilhamento, transferência ou tratamento no Brasil.

Os princípios fundamentais da LGPD, como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas, ganham uma dimensão ainda mais crítica quando aplicados aos dados sensíveis.

O princípio da finalidade, por exemplo, adquire uma importância crucial no contexto dos dados sensíveis.

Como destacado por Doneda (2019), este princípio fundamenta a restrição da transferência de dados pessoais a terceiros e estabelece um critério para avaliar a razoabilidade da utilização de dados para uma finalidade específica.

Maria Celina Bodin de Moraes, citando Stefano Rodotà (2008), enfatiza que as razões para a coleta de dados sensíveis devem ser objetivas e limitadas, condicionadas à comunicação prévia ao interessado sobre como as informações serão utilizadas.

O princípio da não discriminação também assume uma relevância especial no tratamento de dados sensíveis.

Embora a LGPD proíba o uso de dados pessoais para fins discriminatórios ilícitos ou abusivos, ela parece permitir tratamentos distintivos que sejam lícitos e não abusivos.

Esta nuance levanta questões importantes sobre o tratamento de dados sensíveis, pois mesmo que um tratamento discriminatório seja considerado lícito e não abusivo para dados pessoais comuns, é questionável se o mesmo se aplicaria aos dados sensíveis, dada sua natureza personalíssima e a necessidade de tutela prioritária.

Rodotà (2018) alerta que a coleta de dados sensíveis e perfis sociais e individuais pode levar à discriminação, argumentando que a privacidade deve ser vista como uma proteção contra o controle público e o estigma social, bem como uma salvaguarda contra a simplificação e objetificação dos indivíduos.

Nesse sentido, o tratamento de dados sensíveis exige uma abordagem ainda mais cautelosa e rigorosa do que a aplicada aos dados pessoais comuns, sempre priorizando a proteção da privacidade e da dignidade do titular dos dados.

O consentimento desempenha um papel crucial no tratamento de dados sensíveis sob a LGPD.

Conforme o artigo 11, inciso I, da lei (BRASIL, 2018), o tratamento de dados sensíveis só poderá ocorrer quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas.

Este requisito reforça a autonomia do titular dos dados e busca garantir que ele esteja plenamente ciente das implicações do compartilhamento de suas informações sensíveis.

À medida que a sociedade enfrenta os desafios crescentes da era digital e da proteção de dados, a interpretação e aplicação destes princípios no contexto dos dados sensíveis continuará a ser um tema de debate e desenvolvimento jurisprudencial.

A LGPD fornece um framework robusto para a proteção de dados pessoais, mas sua eficácia na proteção de dados sensíveis dependerá da rigorosa aplicação de seus princípios e da constante vigilância para garantir que

os direitos fundamentais dos indivíduos sejam respeitados no ambiente digital em rápida evolução.

3.1 TUTELA DOS DIREITOS FUNDAMENTAIS E A PROTEÇÃO DOS DADOS SENSÍVEIS

A Lei Geral de Proteção de Dados (LGPD) estabelece mecanismos robustos para a tutela dos direitos fundamentais no contexto da proteção de dados sensíveis.

Fundamentada no respeito à privacidade, na autodeterminação informativa, e na liberdade de expressão, informação, comunicação e opinião, a LGPD coloca o consentimento como elemento central na proteção de dados sensíveis.

Conforme o artigo 11, inciso I da lei, o consentimento para o tratamento desses dados deve ser específico e destacado, reforçando a autonomia do titular dos dados e buscando garantir que ele esteja plenamente ciente das implicações do compartilhamento de suas informações sensíveis (BIONI; BRUNO, 2019).

A evolução do conceito de privacidade, que passou do simples "direito de ser deixado só" para incluir o controle sobre as próprias informações, reflete-se na abordagem da LGPD.

Segundo Rodotà (2008), que argumenta que a privacidade deve ser considerada como o direito de cuidar das próprias informações.

> O direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular.

Esta perspectiva está alinhada com o princípio da autodeterminação informativa, que é central na LGPD.

O princípio da não discriminação emerge como um pilar fundamental neste contexto, nas palavras de Rodotà (2008, p. 56)

> A formação de perfis baseados em dados pessoais sensíveis pode gerar discriminação [...] seja porque dados pessoais, aparentemente não 'sensíveis', podem se tornar sensíveis se contribuem para a elaboração de um perfil; seja porque a própria esfera individual pode ser prejudicada quando se pertence a um grupo do qual tenha sido traçado um perfil com conotações negativas.

A LGPD, inspirada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR), estabelece restrições específicas para o tratamento de dados sensíveis, reconhecendo a vulnerabilidade intrínseca do titular desses dados.

O tratamento de grandes volumes de dados (big data) apresenta novos desafios à proteção de dados sensíveis.

Cohen (2000) relata casos de discriminação baseada em dados sensíveis, como em seguros de saúde e empréstimos bancários.

Estes exemplos ilustram como o uso inadequado de dados sensíveis pode levar a práticas discriminatórias, reforçando a importância da proteção legal.

A tutela constitucional da igualdade e não-discriminação, da Constituição Federal, presente no artigo 5º, caput (BRASIL, 1988) é reforçada pela LGPD:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> [...]

Como aponta Mendes (2014), no âmbito dos dados sensíveis, a tutela dos direitos fundamentais se manifesta na proteção à dignidade da pessoa humana, na garantia da igualdade, na preservação da privacidade e intimidade, e na liberdade de consciência e crença.

Contudo, a LGPD também prevê exceções à necessidade de consentimento para o tratamento de dados sensíveis em certas situações, como para a execução de políticas públicas. Esta disposição suscita debates sobre a ponderação adequada entre interesses públicos e a proteção de direitos fundamentais individuais (MULHOLLAND, 2020).

Apesar dos avanços significativos representados pela LGPD, sua eficácia na proteção de dados sensíveis ainda enfrenta desafios consideráveis.

Estes incluem questões de implementação prática, a necessidade de fiscalização efetiva, a importância da conscientização contínua dos titulares dos dados, e os desafios tecnológicos em constante evolução.

A superação desses obstáculos será crucial para garantir que a proteção dos dados sensíveis no Brasil seja não apenas robusta na teoria, mas também eficaz na prática, salvaguardando os direitos fundamentais dos cidadãos na era digital.

4 ANPD - AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (LGPD) estabelece a criação da Autoridade Nacional de Proteção de Dados (ANPD), uma entidade fundamental para a implementação e fiscalização da legislação de proteção de dados no Brasil.

A ANPD é um órgão vinculado à Presidência da República, com a responsabilidade de assegurar o cumprimento da LGPD em todo o território nacional, supervisionando o tratamento de dados pessoais realizado por instituições públicas e privadas.

Como destaca Bioni (2019, p. 89), a criação da ANPD é um marco em matéria legislativa, auxiliando a garantir os direitos fundamentais.

> Um passo essencial para assegurar a conformidade com a LGPD e garantir que direitos fundamentais sejam protegidos no contexto do tratamento de dados pessoais.

A existência de uma autoridade específica para a proteção de dados, similar ao que ocorre com o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, visa assegurar uma aplicação uniforme e eficiente das normas de privacidade e segurança de dados.

Sua criação representa um passo significativo na estruturação de um sistema robusto de proteção de dados no Brasil, alinhando o país com as melhores práticas internacionais.

Além de atuar como órgão regulador e fiscalizador, a ANPD desempenha um papel essencial na orientação e conscientização do público, como expressa Pinheiro (2020, p. 55) que enfatiza que, para que a ANPD cumpra seu papel de forma eficaz, é necessário que sua atuação alcance a população, empresas e o setor público:

> Vá além da fiscalização, abrangendo também a conscientização pública e a orientação às empresas e ao setor público.

Isso significa que a ANPD deve promover uma cultura de proteção de dados, educando tanto os titulares quanto os responsáveis pelo tratamento de dados sobre os direitos e deveres previstos pela LGPD.

Outro aspecto relevante é a autonomia da ANPD para atuar sem interferências políticas. Segundo Doneda (2019, p. 78) argumenta que a efetividade da LGPD depende de uma autoridade reguladora independente e com autonomia técnica, de modo a evitar que pressões externas comprometam a proteção dos dados dos cidadãos. A ausência de autonomia pode prejudicar a

aplicação da LGPD, sobretudo no tratamento de dados sensíveis que demandam uma fiscalização mais rigorosa.

A estrutura da ANPD, conforme definida pela LGPD, inclui um Conselho Diretor, órgão máximo de direção, um Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, além de unidades especializadas para a aplicação da lei.

Entre as principais atribuições da ANPD estão a elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais, a fiscalização e aplicação de sanções em casos de descumprimento da lei, a promoção de conhecimento público sobre a proteção de dados, e a realização de auditorias para verificar a conformidade de organizações com a LGPD.

Mendes (2014, p. 102) observa que a proteção de dados depende de uma estrutura de fiscalização robusta que atue de forma preventiva e corretiva. Nesse sentido, a ANPD, ao aplicar as sanções previstas na LGPD, cumpre um papel central não apenas na proteção dos dados pessoais, mas também na promoção da segurança jurídica e da confiança dos cidadãos em um ambiente digital em rápida transformação.

Um aspecto crucial da ANPD é sua competência exclusiva para aplicar as sanções previstas na LGPD, o que centraliza a autoridade regulatória em matéria de proteção de dados.

Esta exclusividade visa garantir uma interpretação uniforme da lei e evitar conflitos de competência com outros órgãos. No entanto, a lei prevê que a ANPD deve articular sua atuação com outros órgãos e entidades que possuam competências relacionadas à proteção de dados.

A questão da autonomia da ANPD tem sido objeto de debate.

Embora a lei declare assegurada a autonomia técnica e decisória do órgão, sua vinculação inicial à Presidência da República levantou preocupações sobre sua independência, especialmente considerando que a ANPD deve regular o tratamento de dados por entidades tanto públicas quanto privadas.

A garantia de uma verdadeira autonomia é vista como essencial para que a ANPD possa cumprir efetivamente seu papel de guardiã da proteção de dados no país.

O estabelecimento e o funcionamento efetivo da ANPD são cruciais para o sucesso da implementação da LGPD.

Sua atuação é fundamental não apenas para a fiscalização e aplicação da lei, mas também para o desenvolvimento de uma cultura de proteção de dados no Brasil.

Através da emissão de diretrizes, realização de estudos e promoção de conhecimento público, a ANPD tem o potencial de moldar significativamente as práticas de proteção de dados no país.

À medida que a ANPD se estabelece e começa a exercer plenamente suas funções, espera-se que ela desempenhe um papel central na interpretação e

aplicação da LGPD, contribuindo para a segurança jurídica e para o equilíbrio entre a inovação tecnológica e a proteção dos direitos fundamentais dos titulares de dados.

O desenvolvimento e a atuação da ANPD nos próximos anos serão, portanto, cruciais para determinar a eficácia do regime de proteção de dados no Brasil e sua capacidade de enfrentar os desafios emergentes na era digital.

Portanto, a criação da ANPD é essencial para a proteção de dados pessoais no Brasil. Sua atuação é fundamental não apenas para a fiscalização e aplicação da lei, mas também para o desenvolvimento de uma cultura de proteção de dados no país, contribuindo para a segurança jurídica e para o equilíbrio entre inovação tecnológica e proteção dos direitos fundamentais dos titulares de dados.

5 IMPACTOS DA LGPD NO TRATAMENTO DE DADOS SENSÍVEIS

A implementação da Lei Geral de Proteção de Dados (LGPD) tem gerado impactos significativos nas práticas de tratamento de dados por parte de empresas e organizações brasileiras, especialmente no que diz respeito aos dados sensíveis.

Estas mudanças são profundas e abrangentes, envolvendo uma revisão completa das políticas de privacidade, a implementação de medidas técnicas e organizacionais de segurança reforçadas, e o desenvolvimento de processos para obtenção e gestão do consentimento específico (TEFFÉ; VIOLA, 2020).

Os desafios enfrentados neste processo são múltiplos e complexos, incluindo a identificação precisa dos dados sensíveis, a gestão eficaz do consentimento, a implementação de medidas de segurança adicionais, e o delicado balanceamento entre utilidade e proteção, particularmente em áreas críticas como saúde e pesquisa científica.

Os impactos da LGPD se estendem para além das práticas organizacionais, afetando esferas econômicas, sociais e tecnológicas.

No âmbito econômico, observam-se custos significativos de adequação para empresas e organizações, embora também se apresentem oportunidades para o desenvolvimento de soluções inovadoras de proteção de dados.

Socialmente, nota-se uma crescente conscientização sobre a importância da privacidade e proteção de dados.

No campo tecnológico, a lei tem impulsionado o desenvolvimento de novas tecnologias de proteção de dados, como criptografia avançada e técnicas de anonimização (TEPEDINO; FRAZÃO; OLIVA, 2020).

O descumprimento das disposições da LGPD, particularmente em relação aos dados sensíveis, pode resultar em consequências severas, incluindo sanções como advertências, multas substanciais, bloqueio ou eliminação dos dados pessoais relacionados à infração (BRASIL, 2018).

Além disso, o vazamento ou uso indevido de dados sensíveis pode desencadear ações de indenização por danos morais e materiais, como evidenciado em decisões recentes dos tribunais brasileiros.

No contexto das relações de consumo, o tratamento inadequado de dados sensíveis pode gerar discriminação e segregação abusiva.

Sendo que Cohen (2000, p. 27) dispõe que nos casos onde exista o tratamento inadequado os dados de consumidores podem ser utilizados para fins com os quais os mesmo não concordem:

> Os dados dos consumidores podem ser utilizados para muitos fins com os quais os consumidores podem não concordar tão alegremente: decisões de emprego e classificações por parte dos prestadores de seguros de saúde que excluem ou prejudicam os “despossuídos” genéticos ou médicos; decisões de emprego ou habitação baseadas em riscos de personalidade percebidos; decisões de emprego ou habitação baseadas em preferências sexuais ou religiosas; e assim por diante.

Esta preocupação ressalta a importância crucial da proteção adequada dos dados sensíveis para prevenir práticas discriminatórias e garantir a igualdade de tratamento em diversos aspectos da vida social e econômica.

6 CASOS RECENTES RELACIONADOS AO VAZAMENTO DE DADOS SENSÍVEIS

Casos recentes de vazamento de dados sensíveis têm destacado a importância da LGPD e os desafios na sua implementação.

Por exemplo, um incidente envolvendo o vazamento de dados de saúde de milhões de pacientes em 2020 ilustrou a vulnerabilidade de sistemas de informação e a necessidade de medidas de segurança robustas (TEPEDINO; FRAZÃO; OLIVA, 2020).

Além desse caso, outros incidentes significativos têm ocorrido globalmente, demonstrando a crescente preocupação com a proteção de dados sensíveis.

Uber (2016) A empresa de aplicativo de transporte sofreu um vazamento de dados que afetou 57 milhões de usuários e motoristas em todo o mundo.

A comunicação sobre o incidente foi realizada apenas após um ano, resultando em severas penalidades. A Uber firmou um acordo de R$500 milhões com os Estados Unidos para encerrar litígios e pagou multas de R$4,5 milhões às autoridades de proteção de dados da Holanda e Reino Unido.

Banco Inter (2018) No Brasil, o Banco Inter enfrentou uma Ação Civil Pública proposta pelo Ministério Público do Distrito Federal e Territórios devido ao vazamento de dados de 19 mil correntistas.

O banco foi acusado de não ter tomado os devidos cuidados para proteger os dados pessoais dos clientes. Inicialmente, houve negativa do incidente e recusa na prestação de informações.

O caso foi encerrado com um acordo de R$1,5 milhão, revertido para instituições de caridade e de combate ao crime cibernético.

Segundo Cohen (2000), a exposição de dados financeiros pode gerar discriminação e prejuízos econômicos aos indivíduos afetados, demonstrando a urgência de medidas protetivas eficazes.

Estes casos ilustram a importância da comunicação rápida e transparente em caso de incidentes de segurança, conforme previsto no artigo 48 da LGPD:

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
>
> § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
>
> I - a descrição da natureza dos dados pessoais afetados;
>
> II - as informações sobre os titulares envolvidos;
>
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
>
> IV - os riscos relacionados ao incidente;
>
> V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
>
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
>
> § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
>
> I - ampla divulgação do fato em meios de comunicação; e
>
> II - medidas para reverter ou mitigar os efeitos do incidente.
>
> § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados

> ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

A lei exige que o controlador comunique à ANPD e ao titular dos dados sobre a ocorrência de incidente de segurança capaz de ocasionar risco ou dano relevante, em "prazo razoável".

A comunicação deve incluir informações sobre a natureza dos dados afetados, os titulares envolvidos, as medidas de segurança adotadas, os riscos envolvidos e as ações para mitigação de prejuízos.

A ANPD tem o poder de determinar medidas adicionais para minimizar as consequências do incidente, incluindo a ampla divulgação do fato em meios de comunicação.

É importante notar que, conforme o artigo 49 da LGPD (BRASIL, 2018), os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados para atender aos requisitos de segurança, padrões de boas práticas de governança, e aos princípios gerais previstos na lei:

> Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

O não cumprimento das disposições da LGPD, especialmente em relação aos dados sensíveis, pode resultar não apenas em responsabilidade civil, mas também em sanções administrativas significativas.

Isso evidencia a necessidade de uma mudança fundamental na abordagem ao tratamento de dados por parte de pessoas naturais, jurídicas e órgãos públicos.

Estes casos recentes e as disposições da LGPD ressaltam a importância de uma gestão proativa e responsável dos dados sensíveis, bem como a necessidade de preparação adequada para responder a incidentes de segurança de forma rápida e eficaz.

A implementação da LGPD tem gerado impactos significativos em diversos setores da economia e da sociedade brasileira, sendo possível, analisar como a lei tem afetado especificamente os setores de saúde, financeiro e recursos humanos.

O setor de saúde lida constantemente com dados sensíveis dos pacientes, o que o torna especialmente vulnerável e, ao mesmo tempo, um alvo crítico para a implementação da LGPD.

Alguns dos principais impactos observados no campo da saúde são o aprimoramento da segurança dos prontuários eletrônicos, os Hospitais e clínicas têm investido em sistemas mais robustos de proteção de dados para garantir a confidencialidade das informações médicas dos pacientes.

A revisão dos processos de consentimento, onde as instituições de saúde têm reformulado seus formulários e procedimentos para obter o consentimento explícito dos pacientes para o tratamento de seus dados de saúde.

Além da maior cautela aplicada no compartilhamento de informações, a troca de informações entre profissionais de saúde e instituições tem se tornado mais criteriosa, buscando equilibrar a necessidade de colaboração médica com a proteção da privacidade dos pacientes.

Um estudo conduzido em hospitais brasileiros indicou que, embora a maioria das instituições tenha feito esforços para se adequar à LGPD, muitas ainda enfrentam desafios significativos, especialmente em relação ao gerenciamento do consentimento para o tratamento de dados sensíveis de saúde (SERPRO, 2019).

Com relação ao setor financeiro, que já estava sujeito a regulamentações rígidas de segurança de dados, também tem sido impactado pela LGPD.

Alguns dos principais efeitos observados são, o aprimoramento dos sistemas de prevenção a fraudes as Instituições financeiras têm investido em tecnologias mais avançadas para proteger os dados sensíveis de seus clientes contra ameaças cibernéticas.

Dentre outras mudanças ocorridas está a revisão das práticas de credit scoring, onde as instituições têm reavaliado seus modelos de análise de crédito para evitar discriminação baseada em dados sensíveis, como raça ou orientação sexual.

Além das práticas demonstradas, o setor financeiro tem empregado práticas que visam maior transparência nas políticas de privacidade, onde os bancos e outras instituições financeiras têm atualizado e simplificado suas políticas de privacidade para torná-las mais compreensíveis aos clientes.

Importante mencionar, o setor de Recursos Humanos (RH) que lida com uma grande quantidade de dados sensíveis dos funcionários, o que o torna um alvo importante para a implementação da LGPD.

Sendo alguns dos principais impactos observados na revisão dos processos de recrutamento e seleção, as empresas têm adaptado seus procedimentos para coletar apenas os dados estritamente necessários dos candidatos, evitando a coleta excessiva de informações sensíveis.

Além de estarem adotando maior cautela no armazenamento de dados dos funcionários, as organizações têm investido em sistemas mais seguros para armazenar informações sensíveis dos colaboradores, como dados de saúde e informações financeiras.

Realizando implementações de políticas de retenção e exclusão de dados, as empresas têm desenvolvido políticas claras sobre por quanto tempo os dados dos funcionários serão mantidos e quando serão excluídos.

7 DAS SANÇÕES PREVISTAS NA LGPD

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n.º 13.709/2018, prevê um conjunto de sanções administrativas aplicáveis às organizações que desrespeitarem suas diretrizes e compromissos com a proteção de dados.

Essas sanções, delineadas no artigo 52 da LGPD, variam em gravidade e natureza, abrangendo desde advertências até multas significativas, sendo todas de competência da Autoridade Nacional de Proteção de Dados (ANPD).

Na visão de Mulholland (2020, p. 142), as sanções da LGPD exercem um papel fundamental na proteção de dados, pelo fato de estabelecerem consequências as práticas inadequadas:

> As sanções da LGPD desempenham um papel central na promoção de uma cultura de proteção de dados, pois estabelecem consequências claras e proporcionais para práticas inadequadas, reforçando a confiança dos titulares de dados.

Entre as penalidades, a LGPD inicia com a advertência, que pode ser emitida com prazo para a adoção de medidas corretivas necessárias.

Outra sanção frequente é a multa simples, que pode chegar a até 2% do faturamento da empresa infratora, limitada a R$ 50 milhões por infração, é uma das penalidades mais severas previstas pela lei e destaca o compromisso do legislador com a proteção dos direitos fundamentais dos cidadãos, e, em casos específicos, também é prevista uma multa diária, respeitando o teto imposto pela multa simples.

A lei também contempla sanções de caráter mais restritivo, como a publicização da infração, mediante a qual a ANPD confirma e expõe a violação cometida, visando conscientizar o público e desencorajar novas infrações.

Além disso, a possibilidade de bloqueio ou eliminação de dados pessoais utilizados em desconformidade com a LGPD demonstra a preocupação com a correção imediata das falhas.

Sobre o tema Bioni (2019, p. 94), menciona que a aplicação de sanções como o bloqueio ou a exclusão de dados é uma forma de assegurar que os danos

causados sejam mitigados e que as organizações reavaliem suas práticas de tratamento.

Para casos de maior gravidade, a LGPD permite sanções ainda mais rígidas, como a suspensão parcial ou total do funcionamento do banco de dados por até seis meses, prorrogável pelo mesmo período, e a suspensão do exercício da atividade de tratamento de dados pessoais por igual duração.

Em situações extremas, é autorizada a proibição total ou parcial do exercício de atividades relacionadas ao tratamento de dados.

A aplicação dessas sanções é guiada pelos princípios de proporcionalidade e razoabilidade, de modo que a ANPD considera aspectos como a gravidade da infração, a boa-fé do infrator, qualquer vantagem obtida, a reincidência, a colaboração com as autoridades e os danos provocados.

Acerca da atuação da Autoridade Nacional de Proteção de Dados (ANPD) Doneda (2019, p. 102) observa que é crucial nesse processo, uma vez que a entidade é responsável por aplicar as sanções previstas na LGPD e promover a conscientização das organizações:

> A ANPD deve equilibrar o rigor na aplicação de penalidades com a promoção de medidas educativas, ajudando as empresas a implementar boas práticas de proteção de dados.

. Essa abordagem dual contribui para que as penalidades sejam não apenas um mecanismo punitivo, mas também preventivo.

Importante observar que as sanções da LGPD não afastam a possibilidade de outras responsabilizações, sejam civis, penais ou administrativas, previstas em normas legais correlatas.

Além disso, a LGPD exige que a ANPD defina, em regulamento próprio, as metodologias para o cálculo das sanções, inclusive o valor-base das multas.

Este regulamento deve ser submetido à consulta pública, assegurando a transparência e o engajamento social na formulação das regras.

Sobre o tema Pinheiro (2020, p. 63) destaca que a consulta pública exigida pela LGPD para a formulação das regras sobre multas e sanções reforça a legitimidade do processo e assegura que as partes interessadas tenham voz.

Essa exigência é fundamental para criar um ambiente de conformidade colaborativa e justo.

Assim, a LGPD impõe às empresas a responsabilidade de seguir rigorosamente seus princípios e dispositivos, promovendo um ambiente em que o tratamento de dados respeite direitos fundamentais e princípios de privacidade, garantindo uma relação de confiança e conformidade entre as organizações e os titulares dos dados.

As sanções previstas pela LGPD representam, portanto, um avanço significativo na regulamentação do tratamento de dados no Brasil. Sua aplicação adequada, aliada a ações educativas, é essencial para garantir a proteção dos dados pessoais e sensíveis e promover uma cultura de responsabilidade no tratamento de informações no país.

8 PERSPECTIVAS FUTURAS E DESAFIOS DA PROTEÇÃO DE DADOS NO BRASIL

A proteção de dados é um campo dinâmico e em constante transformação, profundamente influenciado por tendências globais e avanços tecnológicos. À medida que o cenário digital evolui, a Lei Geral de Proteção de Dados (LGPD) precisará adaptar-se para responder aos novos desafios impostos por tecnologias emergentes e pela crescente integração digital em várias esferas da sociedade.

Esse contexto global de inovação tecnológica e expansão das legislações de proteção de dados demanda atenção a diversas perspectivas futuras, incluindo a regulamentação da inteligência artificial (IA), o aumento de dispositivos conectados pela Internet das Coisas (IoT) e a harmonização das normas de proteção de dados entre diferentes países.

Na visão de Bioni (2019, p. 145), a regulamentação da IA surge como um desafio central, sendo necessária a criação de medidas regulatórias que promovam tanto a inovação quanto a proteção dos direitos fundamentais:

> A utilização crescente de algoritmos de aprendizado de máquina e dispositivos conectados cria novos riscos à privacidade e exige uma abordagem regulatória que promova tanto a inovação quanto a proteção de direitos fundamentais.

A transparência no uso de algoritmos e a mitigação de vieses discriminatórios são aspectos que demandam atenção especial na proteção de dados.

Ferramentas como o Chat GPT, que utilizam dados para aprendizado de máquina, ilustram as complexidades de proteger a privacidade dos usuários e

evitar vieses nos processos algorítmicos. Portanto, a LGPD precisará ser revisitada e adaptada para abordar os desafios específicos trazidos pela IA, garantindo a proteção dos dados enquanto favorece a inovação responsável.

Esse movimento pode incluir exigências de transparência algorítmica, auditorias de sistemas e o direito dos usuários de entender como seus dados são processados.

Segundo Doneda (2019, p. 121), a conscientização dos titulares de dados e a educação das organizações sobre os princípios da LGPD são essenciais para garantir a eficácia da legislação no longo prazo. Isso exige esforços conjuntos da Autoridade Nacional de Proteção de Dados (ANPD), empresas, órgãos públicos e sociedade civil.

Além disso, a ANPD precisará consolidar sua atuação e assegurar recursos suficientes para enfrentar os desafios. Pinheiro (2020, p. 88) destaca que a autonomia financeira e administrativa da ANPD é fundamental para que ela possa exercer sua função de forma independente e eficaz, especialmente diante do aumento exponencial de casos de violação de dados.

No contexto da IoT, a proliferação de dispositivos conectados como assistentes virtuais, câmeras inteligentes e dispositivos de monitoramento de saúde, traz uma complexidade inédita à coleta e ao processamento de dados pessoais. A LGPD pode necessitar de atualizações para incluir diretrizes específicas para proteger dados em ambientes onde a troca de informações é constante e o controle pelo usuário é reduzido.

Essas atualizações podem envolver o fortalecimento de mecanismos de consentimento e a implementação de medidas de segurança adicionais para prevenir vulnerabilidades nos sistemas interconectados.

A evolução da proteção de dados também deve estar intrinsecamente ligada à ética digital. Rodotà (2008, p. 56) argumenta que o respeito à dignidade humana no ambiente digital exige não apenas a proteção contra abusos, mas também a promoção de uma sociedade mais justa e inclusiva, onde a privacidade seja vista como um direito inalienável. Essa perspectiva reforça a necessidade de uma abordagem equilibrada, que contemple avanços tecnológicos e os direitos fundamentais dos indivíduos.

Segundo Bioni e Mendes (2019, p. 173) outro desafio importante é a harmonização entre diferentes regimes de proteção de dados. Com o aumento das legislações de proteção de dados ao redor do mundo, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, torna-se essencial buscar maior compatibilidade entre esses regimes para viabilizar o fluxo transfronteiriço de dados:

> O alinhamento da LGPD com legislações internacionais é essencial para posicionar o Brasil como um ator confiável no cenário global de proteção de dados.

Diante desses desafios, algumas propostas para aprimorar a LGPD incluem o fortalecimento da ANPD e a criação de programas de educação pública para conscientizar a população sobre seus direitos. Quanto mais informada a população estiver, melhor poderá exercer controle sobre seus dados e exigir proteção. O incentivo governamental à adoção de tecnologias avançadas, como criptografia de ponta a ponta e anonimização de dados, também é crucial.

Cots e Oliveira (2020, p. 77) sugerem que regulamentações específicas para áreas como saúde e finanças podem ajudar a mitigar os riscos associados ao grande volume de dados sensíveis tratados nesses setores.

A ética na era dos dados continua sendo um aspecto central. Mendes (2014, p. 89) destaca que fortalecer a capacidade das pessoas de controlar efetivamente seus dados envolve aspectos legais, educacionais e tecnológicos, sendo necessário um esforço conjunto para empoderar os titulares de dados.

Além disso, a cooperação internacional será fundamental para enfrentar os desafios globais de proteção de dados.

Essas considerações reforçam que a proteção de dados deve acompanhar o ritmo da inovação tecnológica e responder aos desafios de um mundo cada vez mais interconectado e dependente da informação digital.

CONSIDERAÇÕES FINAIS

O presente estudo evidenciou que a Lei Geral de Proteção de Dados (LGPD) representa um marco regulatório robusto e essencial para a proteção de dados pessoais sensíveis no Brasil, alinhando-se às melhores práticas internacionais. Contudo, sua efetiva implementação ainda enfrenta desafios, especialmente no que tange à adaptação de empresas e organizações públicas e privadas às exigências legais.

Verificou-se que os dados sensíveis, devido ao seu potencial de causar danos irreparáveis aos titulares, requerem uma atenção redobrada em termos de segurança e consentimento.

A LGPD busca assegurar que esses dados sejam tratados com um rigor específico, garantindo a proteção dos direitos fundamentais, como a privacidade, dignidade e a não discriminação.

No entanto, a aplicabilidade da LGPD ainda depende de um processo contínuo de conscientização e adaptação, tanto por parte das empresas, que precisam revisar suas práticas, quanto por parte dos titulares dos dados, que devem ser informados sobre seus direitos.

A criação da Autoridade Nacional de Proteção de Dados (ANPD) se mostrou crucial para a fiscalização e aplicação das sanções previstas na lei, mas sua atuação precisa ser constantemente fortalecida.

Por fim, conclui-se que, apesar dos avanços proporcionados pela LGPD, o cenário digital impõe desafios dinâmicos e em constante evolução.

A necessidade de aprimoramento contínuo, com foco nas tendências globais, como a regulamentação de tecnologias emergentes, é imperativa para que a proteção dos dados sensíveis se mantenha efetiva e alinhada aos direitos fundamentais dos indivíduos na era digital.

REFERÊNCIAS

AUSTRALIAN RED CROSS BLOOD SERVICE. **Blood Service apologises for donor data leak**. 2016. Disponível em: <https://www.lifeblood.com.au/news-and-stories/media-centre/media-releases/blood-service-apologises-donor-data-leak#:~:text=The%20Australian%20Red%20Cross%20Lifeblood,accessed%20by%20an%20unauthorised%20person.> Acesso em: 25 de set. 2024.

BANCO INTER. **acordo destinará R$1,5 milhão para caridade e combate a crimes cibernéticos. MPDFT**. 19 dez 2018. Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2018/10524-2018-12-19-10-27-31. Acesso em: 25 de set. 2024.

BIONI, B. R. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BIONI, B. R.; MENDES, L. S. **Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência**. Revista de Direito do Consumidor, v. 124, p. 157-180, 2019.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 02 mar 2024.

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, 15 ago. 2018. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 02 de mar 2024.

BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1.758.799/MG. Relator: Min. Nancy Andrighi. Julgado em: 12/11/2019. DJe: 19/11/2019. Disponível em https://processo.stj.jus.br/SCON/jurisprudencia/toc.jsp?livre=%28RESP.clas.+e+%40num%3D%221758799%22%29+ou+%28RESP+adj+%221758799%22%29.suce. Acesso em 15 de jun 2024.

CADWALLADR, C.; GRAHAM-HARRISON, E. **Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach**. The Guardian, 17 mar. 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em: 25 de set. 2024.

COHEN, Julie. **Examined Lives: Informational Privacy and the Subject as Object**. 52 Stan. L. Rev. 1373-1438 (2000).

COTS, M.; OLIVEIRA, R. **Comentários à Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil, 2020.

DONEDA, D. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

FUSSELL, S. **A sex toy company is suing the New York subway for censorship**. The Atlantic, 17 jan. 2017. Disponível em: https://www.theatlantic.com/technology/archive/2017/01/dame-products-subway-ads/513248/. Acesso em: 25 de set. 2024.

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

MULHOLLAND, C. (Coord.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago Editorial, 2020.

PINHEIRO, P. P. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. 2. ed. São Paulo: Saraiva, 2020.

RODOTÀ, S. **A vida na sociedade da vigilância: a privacidade hoje**. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SERPRO. **Serviço Federal de Proteção de Dados. LGPD e saúde: os fins justificam os meios?** 2019. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2019/paciente-no-comando-lgpd-dados-sensiveis-saude. Acesso em: 20 set. 2024.

SCHREIBER, Anderson. **Direitos da Personalidade**. 3 ed. São Paulo: Atlas, 2014.

TEFFÉ, C. S.; VIOLA, M. **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**. Civilistica.com, v. 9, n. 1, p. 1-38, 2020.

TEPEDINO, G.; FRAZÃO, A.; OLIVA, M. D. (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

UBER. **Uber admite que omitiu ataque hacker que roubou dados de 57 milhões de usuários em 2016**. G1, 21 nov 2017. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/uber-admite-ter-sido-alvo-de-ataque-hacker-que-roubou-dados-de-57-milhoes-de-usuarios-em-2016.ghtml. Acesso em: 25 de set. 2024.

UNIÃO EUROPEIA. GDPR – **General Data Protection Regulation**. Of the Regulation (EU) 2016 of the, 04.05.2016. Disponível em: https://www.legislation.gov.uk/eur/2016/679/contents. Acesso em: 20 de abr 2024.