UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

LEI GERAL DE PROTEÇÃO DE DADOS E O DIREITO À PRIVACIDADE DO CONSUMIDOR

ORIENTANDO: Samuel Fellipe da Costa
ORIENTADOR: Prof. Dr. José Carlos de Oliveira

GOIÂNIA
2025

SAMUEL FELLIPE DA COSTA

LEI GERAL DE PROTEÇÃO DE DADOS E O DIREITO À PRIVACIDADE DO CONSUMIDOR

Projeto de Artigo Científico apresentado à disciplina Trabalho de Curso II da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUC GOIÁS).
Prof. Orientador: Dr. José Carlos de Oliveira

GOIÂNIA
2025

SAMUEL FELLIPE DA COSTA

LEI GERAL DE PROTEÇÃO DE DADOS E O DIREITO À PRIVACIDADE DO CONSUMIDOR

Data da Defesa: ____ de _____ de _____

BANCA EXAMINADORA

_____

Orientador: Prof. Dr. José Carlos de Oliveira

_____

Examinador Convidado: Prof. Dr. Luiz Henrique de Almeida

RESUMO

A proteção de dados pessoais tornou-se um tema central no cenário global, especialmente com o avanço da tecnologia e a crescente digitalização das relações sociais e comerciais. No Brasil, a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, surgiu como resposta a essa demanda, estabelecendo diretrizes para o tratamento de dados pessoais e reforçando o direito à privacidade dos cidadãos. Esta pesquisa tem como objetivo analisar a LGPD em seu contexto histórico, jurídico e prático, com foco especial no direito à privacidade do consumidor. Além disso, busca-se contribuir para o debate sobre a importância da privacidade como um direito fundamental em um mundo cada vez mais conectado. Para tanto, adota-se uma metodologia dedutiva, baseada na legislação, doutrinas e artigos. Busca-se, ao final, contribuir para o aprimoramento da compreensão e aplicação da LGPD na proteção efetiva dos direitos dos consumidores no Brasil.

Palavras-chave**:** LGPD; Privacidade; Consumidor; Proteção de Dados; ANPD.

SUMÁRIO

INTRODUÇÃO.....6

1. LEI GERAL DE PROTEÇÃO DE DADOS.....7

1.1 CONTEXTO HISTÓRICO E INTERNACIONAL DA PROTEÇÃO DE DADOS.....7

1.2 CONCEITO E DISPOSIÇÕES DA LGPD.....8

1.3 APLICAÇÃO MATERIAL E TERRITORIAL.....10

2. TRATAMENTO DE DADOS E SEGURANÇA DA INFORMAÇÃO.....11

2.1 PRINCÍPIOS DO TRATAMENTO DE DADOS.....11

2.2 TRATAMENTO DE DADOS PESSOAIS.....14

2.3 TRATAMENTO DE DADOS SENSÍVEIS.....15

2.4 TRATAMENTO DE DADOS PELO PODER PÚBLICO.....16

3. LGPD E O DIREITO À PRIVACIDADE DO CONSUMIDOR.....17

3.1 O PAPEL DA AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD).....19

3.2 FISCALIZAÇÃO E APLICAÇÃO DE SANÇÕES PELA ANPD.....19

CONCLUSÃO.....21

REFERÊNCIAS BIBLIOGRÁFICAS.....23

LEI GERAL DE PROTEÇÃO DE DADOS E O DIREITO À PRIVACIDADE DO CONSUMIDOR

Samuel Fellipe da Costa

INTRODUÇÃO

A proteção de dados pessoais tornou-se um tema de extrema relevância no cenário contemporâneo, especialmente diante do avanço tecnológico e da crescente digitalização das relações sociais e econômicas. No Brasil, a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) representa um marco regulatório fundamental, estabelecendo diretrizes para o tratamento de informações pessoais e reforçando o direito à privacidade, inclusive no âmbito das relações de consumo.

Este trabalho tem como objeto de estudo a análise da LGPD e sua interação com o direito à privacidade do consumidor, abordando seus princípios, aplicações e desafios na prática jurídica.

O objetivo geral desta pesquisa é examinar como a LGPD assegura a proteção dos dados pessoais do consumidor, destacando sua relação com o Código de Defesa do Consumidor (CDC) e o papel da Agência Nacional de Proteção de Dados (ANPD) na fiscalização e aplicação das normas.

O trabalho está estruturado em três tópicos principais. No primeiro, aborda-se o contexto histórico e internacional, conceito, disposições gerais da LGPD e os princípios que regem a proteção de dados. O segundo tópico, discute-se o tratamento de dados e as medidas de segurança da informação. O terceiro, por fim, é voltado para a atuação da Autoridade Nacional de Proteção de Dados (ANPD), com foco na fiscalização e aplicação de sanções, além da análise do impacto da lei na preservação da privacidade do consumidor.

Quanto à metodologia, adota-se uma abordagem qualitativa, baseada em pesquisa bibliográfica e documental, com análise de legislações e jurisprudências pertinentes.

A relevância deste estudo reside na necessidade de compreender os mecanismos legais que protegem a privacidade do consumidor na era digital, bem como os obstáculos para a efetiva implementação da LGPD.

Ao final, espera-se contribuir para o debate sobre a proteção dos dados pessoais no Brasil e destacar a importância do cumprimento efetivo da LGPD como mecanismo de fortalecimento da cidadania digital e da defesa dos consumidores em uma sociedade cada vez mais conectada.

1. LEI GERAL DE PROTEÇÃO DE DADOS

1.1. CONTEXTO HISTÓRICO E INTERNACIONAL DA PROTEÇÃO DE DADOS

A história da proteção de dados pessoais no cenário internacional mostra uma trajetória moldada pelo avanço da tecnologia e pelo aumento da preocupação com a privacidade e segurança das informações. Desde o surgimento dos primeiros sistemas de armazenamento digital, a partir da metade do século XX, governos e instituições começaram a identificar os riscos que o uso massivo de dados poderia representar para os direitos individuais.

Esse debate foi formalizado pela primeira vez nos anos 1970, quando países como a Alemanha e a Suécia começaram a implementar regulamentações específicas sobre proteção de dados. A Suécia, em 1973, criou a primeira legislação de proteção de dados, e a Alemanha seguiu o exemplo com sua Lei Federal de Proteção de Dados, em 1977. Esse movimento foi impulsionado pela expansão do uso de dados em setores como o financeiro e o governamental e pela crescente percepção de que o armazenamento digital poderia ameaçar a privacidade sem regras claras.

Com a globalização e a crescente interconexão dos mercados na década de 1980, surgiram novos desafios para a proteção de dados, uma vez que informações pessoais passaram a ser trocadas entre diferentes países. Em 1980, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) estabeleceu diretrizes sobre a privacidade e os fluxos transnacionais de dados, recomendando princípios como a limitação da coleta e o uso justo dos dados. Essas diretrizes exerceram influência sobre a formulação de leis em diversos países e serviram como um referencial para futuras regulamentações.

Nos anos 1990, com o crescimento do mercado digital, a União Europeia (UE) assumiu um papel de liderança ao introduzir a Diretiva de Proteção de Dados 95/46/EC, em 1995. A proposta visava harmonizar as leis entre os países da UE, garantindo a livre circulação de informações e exigindo que países fora da UE adotassem padrões de proteção compatíveis para poderem manter relações comerciais. Essa diretiva foi um marco importante, inspirando legislações em diversas nações, como Canadá, Austrália, Japão e, mais tarde, o Brasil.

De acordo com Pinheiro (2018, p. 13), o motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização.

Em 2016, a UE aprovou o Regulamento Geral de Proteção de Dados (GDPR), considerado até então a legislação mais completa e rigorosa em matéria de proteção de dados. O GDPR introduziu regras específicas para o tratamento, armazenamento e transferência de dados pessoais e determinou penalidades severas para o descumprimento. O caráter extraterritorial da norma passou a exigir que empresas de fora da UE também se adequassem, impactando legislações ao redor do mundo, inclusive no Brasil, onde foi aprovada a Lei Geral de Proteção de Dados (LGPD) em 2018.

1.2 CONCEITO E DISPOSIÇÕES DA LGPD

Embora as leis de proteção de dados tenham se iniciado internacionalmente na década de 1970, o Brasil deu uma resposta mais tardia a essa questão. Em 1990, com a promulgação do Código de Defesa do Consumidor, o país passou a demonstrar preocupação com a privacidade dos consumidores, estabelecendo o sigilo das informações pessoais dos titulares.

A partir de 2011, surgiram legislações como a Lei do Cadastro Positivo (Lei nº 12.414/2011), que regulamenta os bancos de dados para histórico de crédito e define os direitos dos titulares. Também foi instituída a Lei de Acesso à Informação (Lei nº 12.527/2011), que reforça a importância de um tratamento adequado das informações

pessoais. Em 2012, foi promulgada a Lei Carolina Dieckmann (Lei nº 12.737/2012), que tipifica crimes cibernéticos, incluindo a divulgação não autorizada de dados.

Mais tarde, em 2013, o Brasil aprovou o Marco Civil da Internet (Lei nº 12.965/2014). Esta lei assegura expressamente o direito dos usuários à privacidade e ao sigilo de suas informações pessoais, exceto quando houver consentimento do titular. No entanto, suas disposições ainda eram consideradas limitadas, especialmente quando comparadas às legislações internacionais.

Devido às lacunas presentes no Marco Civil da Internet, tornou-se necessária a formulação de uma lei atualizada e completa: a Lei Geral de Proteção de Dados (LGPD).

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, é a principal legislação brasileira voltada para a regulamentação do tratamento de dados pessoais. Veja-se o que dispõe o art. 1°:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Segundo Lima (2020, p. 36-37), a legislação é um marco divisor de águas diante de inúmeras ocorrências de invasão de privacidade, de vazamentos divulgados com frequência, e tantos outros artifícios utilizados para lucrar com os dados pessoais que se expandiram exponencialmente. Os dados estruturados transformam-se em informação - um dos principais ativos de qualquer atividade econômica e empresarial. A análise de dados pode ser aplicada lucrativamente a tudo no planeta, e sempre será capaz de apresentar informações relevantes para quem as detém.

O art. 2º da Lei Geral de Proteção de Dados Pessoais - LGPD, expressa os seguintes fundamentos:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I - o respeito à privacidade;
>
> II - a autodeterminação informativa;
>
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
>
> IV - a inviolabilidade da intimidade, da honra e da imagem;
>
> V - o desenvolvimento econômico e tecnológico e a inovação;

> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Em síntese, os princípios da LGPD não são meras abstrações legais, mas ferramentas concretas para construir um ecossistema digital mais justo e seguro. Eles refletem a compreensão de que a privacidade é um direito indivisível da dignidade humana, conforme assegurado pela Constituição Federal (art. 5º, X). Como bem sintetiza Pinheiro (2020, p. 68), proteger dados é, em última instância, proteger pessoas. A efetividade da LGPD, portanto, dependerá não apenas da fiscalização da ANPD, mas da internalização desses princípios como valores éticos por toda a sociedade.

1.3 APLICAÇÃO MATERIAL E TERRITORIAL

A LGPD é aplicável a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país no qual estejam localizados os dados, desde que a operação de tratamento de dados seja realizada no Brasil; a atividade de tratamento tenha por objetivo a oferta de bens ou serviços ou o manejo de dados de indivíduos localizados no país; ou, ainda, que os dados pessoais objeto do tratamento tenham sido coletados em território nacional.

A lei se aplica a todos aqueles que realizam o tratamento de dados pessoais, sejam organizações públicas ou privadas, pessoas físicas ou jurídicas, que realizam qualquer operação de tratamento de dados pessoais, independentemente do meio, que possa envolver pelo menos um dos seguintes elementos: (i) ocorrer em território nacional; (ii) que tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; (iii) em que os dados tenham sido coletados no território nacional. (Pinheiro, 2020, p. 26).

Entretanto, estão excluídos da aplicação da lei alguns meios de tratamentos de dados, a exemplo daqueles realizados para fins exclusivamente jornalísticos, artísticos e acadêmicos, além de informações relacionadas exclusivamente à segurança pública, defesa nacional, segurança do Estado e a atividades de investigação e repressão de infrações penais.

2. TRATAMENTO DE DADOS E SEGURANÇA DA INFORMAÇÃO

A Lei Geral de Proteção de Dados (LGPD) estabelece normas para o tratamento de dados pessoais, abrangendo tanto meios físicos quanto digitais. Sua aplicação se estende a pessoas naturais e jurídicas, sejam elas de direito público ou privado, com a finalidade de resguardar direitos fundamentais, como a liberdade, a privacidade e o desenvolvimento pleno da personalidade do indivíduo. Além disso, a LGPD (Art. 5º, X) define "tratamento" como:

> 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.

Assim, a implementação de medidas técnicas e administrativas eficazes é indispensável para prevenir incidentes, fortalecer a confiança nas relações digitais e garantir a conformidade legal no manejo dessas informações.

2.1 PRINCÍPIOS DO TRATAMENTO DE DADOS

A regulamentação de proteção de dados pessoais é uma legislação principiológica, como já foi dito. Sendo assim, tanto na origem europeia como na versão nacional traz um rol de princípios que precisam ser atendidos. A melhor forma de analisar a lei é pela verificação da conformidade dos itens de controle, ou seja, se o controle não está presente, aplicado e implementado, logo o princípio não está atendido

Portanto, a legislação visa fortalecer a proteção da privacidade do titular dos dados, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento econômico e tecnológico.

Pela LGPD, as atividades de tratamento legítimo, específico e explícito de dados pessoais informado previamente ao titular devem estar orientadas pelos seguintes princípios: da finalidade, adequação, necessidade, livre acesso, transparência, segurança, responsabilização e prestação de contas.

A Lei Geral de Proteção de Dados (LGPD), em seu artigo 6º estabelece os princípios que devem reger o tratamento de dados pessoais. Esses princípios são fundamentais para garantir que as atividades de coleta, armazenamento e uso de informações sejam realizadas de forma ética, transparente e alinhada aos direitos dos titulares. Vejamos o que diz o art. 6° e, em seguida, uma breve explanação do princípio abordado:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

O tratamento deve ter um propósito legítimo, específico e explícito, comunicado ao titular. Não é permitido desviar os dados para finalidades incompatíveis com as originalmente informadas. Como explica Doneda (2019, p. 72), a finalidade é a âncora que evita o uso arbitrário de dados, garantindo previsibilidade ao titular.

> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

Na adequação, as operações de tratamento devem ser compatíveis com as finalidades declaradas. Isso implica que os dados coletados devem ter relação direta com o objetivo proposto. Por exemplo, uma empresa não pode coletar dados biométricos para um simples newsletter.

> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

Na necessidade, o tratamento deve limitar-se ao mínimo necessário para atingir a finalidade. Segundo Pinheiro (2020, p. 94), a LGPD rejeita o acúmulo desnecessário de dados, que aumenta riscos de vazamentos e violações.

> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

No princípio do livre acesso, os titulares têm direito a consultar, de forma gratuita e facilitada, informações sobre o tratamento de seus dados, incluindo a forma, a duração e a integralidade das informações processadas.

> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

Já no princípio da qualidade, os dados devem ser exatos, claros, relevantes e atualizados, de acordo com a necessidade do tratamento. Dados desatualizados ou imprecisos podem gerar decisões injustas, como destacam Lima et al. (2020, p. 58).

> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

Na transparência, as informações sobre o tratamento devem ser claras, precisas e acessíveis, garantindo que o titular compreenda como seus dados são utilizados. Barbosa (2022, p. 33) ressalta que a transparência é a base da confiança entre organizações e titulares. Doneda (2019, p. 89) também ressalta que a transparência não é apenas uma obrigação legal, mas um mecanismo de diálogo entre empresas e cidadãos.

> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

O princípio da segurança ocorre com a adoção de medidas técnicas e administrativas para proteger dados contra acessos não autorizados, perdas ou destruição é obrigatória. A segurança é um princípio que demanda investimentos contínuos, como enfatiza Costa (2022, p. 89).

> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

Na prevenção, as organizações devem adotar medidas para evitar danos decorrentes do tratamento, como políticas de backup e planos de contingência.

> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

A não discriminação proíbe-se o uso de dados para fins discriminatórios, ilícitos ou abusivos. Por exemplo, algoritmos que reforcem viés racial ou de gênero violam esse princípio.

> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Na responsabilização e prestação de contas as empresas devem comprovar a adoção de medidas eficazes para cumprir a LGPD. Esse princípio exige documentação robusta, como políticas internas e registros de auditoria.

Esses princípios não são meras recomendações, mas obrigações legais cujo descumprimento pode resultar em multas de até 2% do faturamento da empresa, conforme explica Pinheiro (2020, p. 72).

No entanto, a aplicação desses princípios enfrenta desafios práticos. Pequenas empresas, por exemplo, muitas vezes desconhecem como implementar o princípio da responsabilização, que exige a documentação de processos e a demonstração de conformidade. Da mesma forma, órgãos públicos enfrentam dificuldades para alinhar o princípio da prevenção com infraestruturas tecnológicas defasadas.

2.2 TRATAMENTO DE DADOS PESSOAIS

A crescente digitalização das relações sociais e comerciais trouxe desafios significativos para a proteção de dados pessoais. Nesse contexto, a Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, emerge como um marco regulatório fundamental para garantir a segurança das informações dos cidadãos. Segundo Doneda (2021), a proteção de dados transcende a esfera individual, alcançando um interesse coletivo e demandando regulação e fiscalização adequadas. O tratamento adequado dos dados e a implementação de medidas de segurança tornam-se essenciais para evitar o uso indevido de informações e resguardar direitos fundamentais, como a privacidade e a liberdade.

De acordo com a lei, um dado pessoal é informação relacionada à pessoa natural identificada ou identificável. Como exemplos: número do CPF, data de nascimento, endereço residencial e e-mail.

2.3 TRATAMENTO DE DADOS SENSÍVEIS

Nos termos do inciso II do art. 5.º da Lei Geral de Proteção de Dados, dados sensíveis são aqueles que versam 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. Inobstante, o § 1.º, art. 11 da LGPD, complementa informando a aplicação da base legal do art. 11 – O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: – quando revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

Merece destaque a passagem de Danilo Doneda (2022, p.24):

> A elaboração desta categoria e de disciplinas específicas a ela aplicadas não foi isenta de críticas, como a que arma que é impossível, em última análise, definir antecipadamente os efeitos do tratamento de uma informação, seja ela da natureza que for. Desta forma, mesmo dados não qualificados como sensíveis, quando submetidos a um determinado tratamento, podem revelar aspectos sobre a personalidade de alguém, podendo levar a práticas discriminatórias. Arma-se, em síntese, que um dado, em si, não é perigoso ou discriminatório – mas o uso que dele se faz pode sê-lo. Deve-se ter em conta que o próprio conceito de dados sensíveis atende à uma necessidade de delimitar uma área na qual a probabilidade de utilização discriminatória da informação é potencialmente maior – sem deixarmos de reconhecer que há situações onde tal consequência pode advir sem que sejam utilizados dados sensíveis, ou então que a utilização destes dados se preste a fins legítimos e lícitos.

Dados sensíveis possuem como característica distintiva dos dados pessoais a presunção de que o tratamento daqueles representam risco, potencial danoso e discriminatório elevados para o titular. Considerados o “núcleo duro da privacidade”, demanda o mais alto grau protetivo.

Ana Frazão salienta que a linha de distinção entre dados pessoais e dados sensíveis, em determinadas hipóteses, pode não ser clara, posto que a perspectiva da análise deve ser dinâmica, jamais estática, acrescentando que são sensíveis todos os dados que permitem que se chegue, como resultado, a informações sensíveis a respeito das pessoas.

2.4 TRATAMENTO DE DADOS PELO PODER PÚBLICO

É fato que a coleta e armazenamento de dados permite ao poder público a criação e efetivação de políticas públicas e a elaboração de serviços públicos mais eficientes e direcionados às necessidades dos cidadãos que contribuem com a qualidade de vida de seus usuários.

De acordo com a Comissão de Direito da Tecnologia e da Informação OAB/PE (CDTI, 2019, P.45) é imprescindível que esse tratamento de dados ocorra dentro de parâmetros éticos e legais. A transparência é um pilar essencial: os cidadãos devem ser informados sobre a finalidade do uso de suas informações, e é necessária a designação de um encarregado para supervisionar o processo, conforme previsto na LGPD. Quando esses critérios são respeitados, o uso de dados públicos se torna não apenas legítimo, mas também estratégico. Afinal, são essas informações que permitem ao Estado aprimorar a infraestrutura urbana em áreas carentes, otimizar a distribuição de recursos educacionais ou até mesmo combater desigualdades sociais. Dessa forma, o tratamento responsável de dados transcende a mera burocracia — transforma-se em um instrumento de promoção do bem-estar coletivo.

> Dado o grande valor dessas informações, a principal preocupação está no risco de que possam ser compartilhadas e utilizadas para fins distintos dos previstos, possibilitando sua exploração econômica pelo setor público e colocando em perigo a privacidade dos cidadãos. Como detentor da maior base de dados da população, o setor público levanta inquietações quanto ao uso indevido dessas informações. Caso sejam manipuladas por agentes mal-intencionados, podem causar sérios prejuízos à sociedade, gerando questionamentos sobre o real compromisso do Estado na proteção dos direitos e garantias individuais. (CDTI OAB/PE, 2019, P.45)

Da mesma forma que as instituições privadas devem apresentar uma finalidade clara e transparente para a realização do tratamento de dados pessoais, a pessoa jurídica de direito público deve adotar a finalidade pública e o interesse público para a realização de tratamento de dados.

Diferentemente das empresas privadas, as instituições públicas poderão seguir os prazos e procedimentos apontados pelas Leis n. 9.507, de 12 de novembro de 1997 (Lei do Habeas Data), n. 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) e n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação). No caso das empresas públicas, o art. 173 da Constituição lhes garante tratamento igual ao reservado às empresas privadas.

> Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.
>
> Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

O artigo 24 estabelece a fundamentação constitucional para o tratamento diferenciado das empresas públicas. A intenção foi criar uma distinção no tratamento de dados pessoais dentro das instituições governamentais, antecipando possíveis cenários futuros, inclusive no que se refere ao cumprimento de outras legislações, como a Lei de Acesso à Informação.

3. LGPD E O DIREITO À PRIVACIDADE DO CONSUMIDOR

A promulgação da Lei Geral de Proteção de Dados (LGPD) trouxe profundas mudanças ao comércio eletrônico e às relações consumeristas, transformando a maneira como as empresas lidam com as informações pessoais de seus clientes. Em um cenário no qual o comércio digital cresce exponencialmente, impulsionado pela coleta de dados para personalização de serviços e estratégias de marketing, a LGPD estabeleceu uma nova dinâmica, impondo limites claros e reforçando os direitos dos consumidores no ambiente digital (BRASIL, 2018).

O impacto mais imediato da LGPD no comércio eletrônico está relacionado à exigência de transparência no tratamento de dados pessoais. Empresas que operam em plataformas digitais precisam fornecer informações claras e acessíveis sobre a finalidade e os métodos de coleta, armazenamento e compartilhamento de dados. Esse princípio, presente no artigo 6º da LGPD, busca corrigir o desequilíbrio informacional que caracteriza as relações entre consumidores e empresas, especialmente em ambientes digitais, onde os usuários frequentemente aceitam termos de uso complexos sem plena compreensão de seu conteúdo (BRASIL, 2018; CUNHA, 2020).

A LGPD exige que o consentimento para a coleta e o uso de dados seja livre, informado e inequívoco, o que exige que empresas adaptem suas políticas de privacidade para garantir a conformidade legal. Por exemplo, o uso de cookies e

outras tecnologias de rastreamento deve ser previamente autorizado pelos consumidores, eliminando práticas como a aceitação tácita e garantindo maior controle sobre os dados compartilhados (FOLLONE; SIMÃO FILHO, 2020).

Além disso, a LGPD ampliou as obrigações das empresas no que se refere à segurança da informação. Plataformas de comércio eletrônico, que lidam com dados financeiros e pessoais sensíveis, são obrigadas a implementar medidas técnicas e administrativas para proteger os dados contra acessos não autorizados e vazamentos, práticas que se tornaram críticas diante do aumento de ciberataques e da sofisticação das técnicas empregadas por criminosos digitais (BRASIL, 2018; HOMCI, 2023). A exigência de relatórios de impacto e de mecanismos de resposta a incidentes também reforça a responsabilidade das empresas, incentivando uma cultura de prevenção e mitigação de riscos.

A integração entre a LGPD e o Código de Defesa do Consumidor (CDC) fortaleceu ainda mais a proteção no comércio eletrônico. Enquanto o CDC já previa direitos como a correção de dados em cadastros e a proteção contra práticas abusivas, a LGPD detalhou procedimentos e responsabilidades no tratamento de dados, ampliando o escopo das obrigações empresariais e assegurando maior segurança jurídica aos consumidores (BRASIL, 1990; FOLLONE; SIMÃO FILHO, 2020).

Os titulares de dados poderão solicitar às empresas, através de simples requerimento, que forneçam, no prazo de 15 dias, informações relativas aos seus dados, devendo constar a indicação da origem dos dados, da finalidade do tratamento, dos critérios utilizados para coleta e tratamento, ou declaração de inexistência de dados, com fundamento nos artigos 9º da LGPD:

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso.

Por sua vez, o Código de Defesa do Consumidor (Lei nº 8.078/90), determina que o consumidor terá acesso as suas informações existentes em cadastros, fichas, registros e dados pessoais e de consumos arquivados sobre ele, bem como as suas respectivas fontes, nos termos do artigo 43 do CDC:

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

A LGPD é condição para o Brasil seguir como participante de uma economia global, já que os países desenvolvidos possuem as suas respectivas leis de proteção de dados. Portanto, as empresas precisam investir em treinamento e conscientização de seus profissionais na realização de um diagnóstico, para estar em conformidade com a LGPD e CDC, a fim de evitarem sanções que podem inviabilizar a continuidade de seus negócios.

3.1 O PAPEL DA AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

A Agência Nacional De Proteção De Dados (ANPD) foi concebida como uma entidade da administração pública federal, vinculada à Presidência da República, com autonomia técnica e decisória. Conforme Doneda (2021, p. 145), a independência funcional da ANPD é crucial para evitar interferências políticas em decisões técnicas, garantindo imparcialidade na aplicação da LGPD.

Sua estrutura inclui um Conselho Diretor, composto por cinco membros nomeados pelo Presidente da República, e uma Diretoria Executiva, responsável pela operacionalização das atividades.

De acordo com o artigo 55-J da LGPD e o Art. 2ª do Decreto 10.474/2020, compete à ANPD elaborar diretrizes para a política nacional de proteção de dados pessoais e da privacidade, fiscalizar e aplicar sanções em casos de descumprimento da legislação, além de orientar agentes de tratamento e a sociedade sobre boas práticas na segurança da informação.

Conforme destaca Pinheiro (2020, p. 215), a ANPD não é um mero ‘policial da LGPD’, mas uma instituição estratégica para a construção de uma cultura de proteção de dados no Brasil. Sua função transcende a punição, abrangendo a mediação de conflitos e a divulgação de boas práticas, em linha com princípios internacionais de governança regulatória.

A ANPD é peça central na efetividade da LGPD, mas seu sucesso depende de maior investimento e aprimoramento de sua autonomia. Como ressalta Pinheiro (2023, p. 201), a autoridade precisa evoluir de um papel sancionador para um agente promotor de inovação responsável. Seus desafios refletem a complexidade de regular

a privacidade em um mundo hiper conectado, onde dados são tanto um ativo quanto uma vulnerabilidade.

3.2 FISCALIZAÇÃO E APLICAÇÃO DE SANÇÕES PELA ANPD

A efetividade de qualquer marco regulatório depende, em grande medida, de mecanismos robustos de fiscalização e de um sistema sancionatório capaz de coibir violações e incentivar a conformidade. No contexto da Lei Geral de Proteção de Dados (LGPD), essa responsabilidade é atribuída à Autoridade Nacional de Proteção de Dados (ANPD), entidade integrante da Presidência da República, criada pelo art. 55-A da Lei nº 13.709/2018. A ANPD assume um papel central na garantia do cumprimento das normas de proteção de dados, atuando não apenas como órgão fiscalizador, mas também como orientador de empresas, órgãos públicos e cidadãos

A atuação da ANPD está alicerçada em competências específicas previstas no art. 55-J da LGPD, que incluem a elaboração de diretrizes, a promoção de ações educativas e a aplicação de sanções administrativas.

Dessa forma, observa-se que a LGPD busca estimular a aplicação de seus dispositivos em caráter preventivo. As sanções vão desde advertências até a imputação de multa simples – que pode chegar a 2% do faturamento, cujo valor fica limitado a um total de R$ 50 milhões – e diária, além da suspensão das atividades relativas ao banco de dados.

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I – advertência, com indicação de prazo para adoção de medidas corretivas;
>
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II – multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

A imputação de sanções administrativas faz com que os entes responsáveis pelo tratamento de dados pessoais atentem-se à garantia da segurança das informações que estão utilizando.

E diferentemente das sanções previstas na LGPD (art. 52 da Lei nº 13.709/2018), a violação dos direitos dos consumidores (Lei nº 8.078/90) constitui infração penal, tendo em vista que impedir ou dificultar o acesso do consumidor, bem como, deixar de corrigir ou lhe entregar informações a seu respeito, configura crime com pena de detenção ou multa, nos termos do artigo 72 e 73 do CDC:

> Art. 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros:
>
> Pena Detenção de seis meses a um ano ou multa.
>
> Art. 73. Deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata:
>
> Pena Detenção de um a seis meses ou multa.

Cabe à autoridade nacional responsável a análise do caso e proporcional aplicação das medidas de sanção. A aplicação deste artigo está pendente da constituição da ANPD, apesar de a vigilância e a fiscalização da lei poderem ser realizadas pelo Ministério Público até que a Autoridade seja constituída.

O art. 53 dispõe:

> Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa.

A análise parte do pressuposto de que a legitimidade da ANPD depende não apenas de seu poder coercitivo, mas de sua capacidade de dialogar com a sociedade e promover a adesão voluntária às normas. Como afirma Lima (2020, p. 89), sanções são necessárias, mas a educação e a transparência são as verdadeiras alavancas da mudança cultural exigida pela LGPD.

4. CONCLUSÃO

A Lei Geral de Proteção de Dados (LGPD), instituída pela Lei nº 13.709/2018, representa um avanço significativo na proteção de direitos fundamentais em um cenário global marcado pela intensa troca de informações e pela dependência tecnológica. Ao longo deste trabalho, buscou-se demonstrar como a legislação

brasileira se alinha a padrões internacionais de privacidade, ao mesmo tempo em que enfrenta desafios específicos decorrentes da realidade socioeconômica do país.

A análise evidenciou que a LGPD não se limita a impor obrigações técnicas e burocráticas às organizações. A privacidade do consumidor é reconhecida como um direito indissociável da dignidade humana. A intersecção entre a LGPD e o Código de Defesa do Consumidor (CDC) reforça essa premissa, ao exigir transparência, boa-fé e equilíbrio nas relações de consumo.

No que tange à segurança da informação, o estudo demonstrou que a adoção de medidas técnicas e administrativas (como políticas internas e treinamentos) não é apenas uma exigência legal, mas uma estratégia essencial para mitigar riscos reputacionais e financeiros. A atuação da Autoridade Nacional de Proteção de Dados (ANPD), por sua vez, mostrou-se fundamental para garantir a efetividade da LGPD, combinando ações educativas com um sistema sancionatório gradual e proporcional.

Contudo, é importante reconhecer que a implementação da LGPD ainda enfrenta obstáculos. A falta de conscientização de pequenas empresas, a escassez de recursos técnicos em órgãos públicos e a necessidade de maior clareza em diretrizes específicas, como o tratamento de dados sensíveis, são desafios que demandam atenção contínua. Como apontado por Pinheiro (2020), a conformidade não é um estado permanente, mas um processo dinâmico que exige adaptação constante.

Em síntese, este trabalho reforça a tese de que a LGPD se consolida como um instrumento de transformação social, capaz de harmonizar inovação tecnológica, desenvolvimento econômico e proteção de direitos individuais. Para que seu potencial seja plenamente realizado é indispensável o engajamento de todos os entes envolvidos (Estado, empresas e cidadãos) na construção de uma cultura de proteção de dados.

Como sugere Lima (2020, p. 132), a privacidade não é um luxo, mas uma condição básica para a liberdade. Nesse sentido, a LGPD não apenas reflete as demandas de um mundo digitalizado, mas também resgata valores essenciais para a convivência democrática, reafirmando que, em última instância, proteger dados é proteger pessoas.

5. REFERÊNCIAS BIBLIOGRÁFICAS

BARBOSA, Mariana. Políticas de Segurança da Informação na Era Digital. São Paulo: Atlas, 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Institui a Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L13709.htm. Acesso em: 08 mar. 2025.

COSTA, Ricardo. Segurança da Informação: Teoria e Prática. Porto Alegre: Bookman, 2022.

CUNHA, Milena. A proteção de dados pessoais nas relações de consumo virtuais. 2020.

DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. 2. ed. São Paulo: Thomson Reuters, 2019.

DONEDA, Danilo. Regulação e Proteção de Dados no Brasil. Rio de Janeiro: Forense, 2021

DONEDA, Danilo. A proteção de dados pessoais nas relações de consumo: para além da informação creditícia. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010; LOPES, Alexandra Krastins et al. Guia orientativo: cookies e proteção de dados pessoais. Brasília: ANPD, out. 2022. p. 24. Disponível em: https://www.gov.br/anpd/ptbr/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-dedados-pessoais.pdf. Acesso em: 08 mar. 2025.

EJUR SOLUÇÕES JURÍDICAS. Proteção de dados no contexto internacional e a origem da LGPD. Disponível em: https://ejur.com.br/blog/a-protecao-de-dados-no-contexto-internacional-e-a-origem-da-lgpd/. Acesso em: 08 mar. 2025.

FRAZÃO, Ana. Nova LGPD: o tratamento dos dados pessoais sensíveis. A quinta parte de uma série sobre as repercussões para a atividade empresarial. Jota, 26 set. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-emercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis26092018. Acesso em: 08 mar. 2025.

FLORENÇO, Larissa Britto. A proteção de dados pessoais nas relações de consumo como um direito fundamental: perspectivas de um marco regulatório para o Brasil. Revista da ESMESC, v. 23, n. 29, p. 165-182, 2016.

FOLLONE, Renata Aparecida; SIMÃO FILHO, Adalberto. A conexão da LGPD e CDC: a proteção de dados pessoais nas relações consumeristas e a sua concretização como direito fundamental. In: Anais do Congresso Brasileiro de Processo Coletivo e Cidadania. 2020.

GUASTINI, Thiago Coelho. Proteção de dados, responsabilidade civil e impactos da LGPD nas relações de consumo. 2023.

HOMCI, Janaina Vieira. A proteção dos dados pessoais no consumo digital. Editora Thoth, 2023.

JIMENE, Camilla do Vale. Capítulo VII: da segurança e das boas práticas. In: MALDONADO, Viviane Nóbrega. BLUM, Renato Opice. (coord). LGPD: Lei Geral de Proteção de Dados. São Paulo: RT, 2019.

JUSBRASIL. Contexto histórico e finalidade da lei geral de proteção de dados. Disponível em: https://www.jusbrasil.com.br/artigos/contexto-historico-e-finalidade-da-lei-geral-de-protecao-de-dados-lgpd/1203647706. Acesso em: 08 mar. 2025.

LIMA, Ana Paula Moraes Canto de, Dionice de Almeida, Eduardo Pereira Maroso. LGPD - Lei Geral de Proteção de Dados [recurso eletrônico]: sua empresa está pronta? - São Paulo, SP: Literare Books International, 2020.

OLIVEIRA, Fernando. Criptografia e Proteção de Dados. Belo Horizonte: Editora Tecnológica, 2021.

PINHEIRO, Patricia Peck Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD) / Patricia Peck Pinheiro. – São Paulo: Saraiva Educação, 2018.

PINHEIRO, Patricia Peck Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD) / Patricia Peck Pinheiro – 2. ed. – São Paulo: Saraiva Educação, 2020.

PINHEIRO, Patricia Peck. ANPD: Avanços e Desafios. 2. ed. São Paulo: Saraiva Educação, 2023.

SUPERIOR TRIBUNAL DE JUSTIÇA. Lei geral de proteção de dados. Disponível em: https://www.stj.jus.br/sites/portalp/Leis-e-normas/lei-geral-de-protecao-de-dados-pessoais-lgpd#:~:text=A%20LGPD%20veda%20ao%20Poder,forem%20acess%C3%ADveis%20publicamente%3B%20quando%20houver. Acesso em 08 mar. 2025.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. Civilistica.com, Rio de Janeiro, v. 9, n. 1, p. 29-30, 2020. Disponível em: http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/. Acesso em: 08 mar. 2025.