

A proteção de dados pessoais como direito humano fundamental: limites ao uso de informações e seus impactos na efetivação dos direitos sociais na era digital

Personal data protection as a fundamental human right: limits on the use of information and its implications for the realization of social rights in the digital age

Bianca Zanin Almeida

Felipe Franco da Fonseca

Guilherme Salvador Alves

Maria Paula Gonçalves Arriero

RESUMO

O presente estudo analisa a proteção de dados pessoais como direito humano fundamental no contexto da sociedade digital, destacando sua importância para a garantia da privacidade, da dignidade humana e dos direitos sociais. Examina a evolução desse direito no ordenamento jurídico brasileiro, com ênfase na Emenda Constitucional nº 115/2022 e na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). O trabalho também aborda os principais princípios e limites jurídicos estabelecidos pela LGPD, evidenciando a necessidade de que o tratamento de dados pessoais ocorra de forma transparente, legítima e segura. Além disso, destaca os mecanismos de responsabilização aplicáveis aos agentes que utilizam informações pessoais em desconformidade com a legislação. Em seguida, discute os impactos do uso de dados pessoais na efetivação dos direitos sociais, demonstrando que o tratamento inadequado dessas informações pode gerar discriminação, vigilância excessiva e exclusão digital, comprometendo a igualdade e o acesso a serviços públicos essenciais. Por outro lado, ressalta que o uso responsável dos dados pode contribuir para o aprimoramento das políticas públicas e da gestão administrativa. Ressalta-se, ainda, que a proteção de dados pessoais não se limita ao cumprimento de normas legais, mas representa condição indispensável para a preservação da confiança nas relações entre cidadãos, Estado e instituições privadas. Nesse sentido, o fortalecimento da cultura de proteção de dados mostra-se essencial para assegurar o exercício

pleno dos direitos fundamentais na sociedade contemporânea. Por fim, conclui que o avanço tecnológico deve ser acompanhado de mecanismos eficazes de proteção de dados, pautados na governança, na transparência e na responsabilidade institucional. Assim, defende a necessidade de conciliar inovação tecnológica com a proteção dos direitos humanos, assegurando a dignidade da pessoa humana e a efetivação dos direitos sociais na sociedade digital.

Palavras-chave: Proteção de dados pessoais; Direitos humanos; Lei Geral de Proteção de Dados (LGPD); Direitos sociais; Sociedade digital.

ABSTRACT

This study analyzes the protection of personal data as a fundamental human right within the context of the digital society, emphasizing its importance for safeguarding privacy, human dignity, and social rights. It examines the evolution of this right in the Brazilian legal system, with particular focus on Constitutional Amendment No. 115/2022 and the Brazilian General Data Protection Law (Law No. 13,709/2018 – LGPD). The research also discusses the main legal principles and limitations established by the LGPD, highlighting the need for personal data processing to be conducted in a transparent, lawful, and secure manner, as well as the accountability mechanisms applicable to violations of data protection regulations. Furthermore, the study addresses the impacts of personal data processing on the effectiveness of social rights, demonstrating that the improper use of personal information may result in discrimination, excessive surveillance, and digital exclusion, thereby undermining equality and access to essential public services. Conversely, it recognizes that the responsible use of data can contribute to improving public policies and administrative efficiency. Finally, the study concludes that technological advancement must be accompanied by effective data protection mechanisms based on governance, transparency, and institutional accountability. It therefore advocates for a balance between technological innovation and the protection of human rights, ensuring respect for human dignity and the effective realization of social rights in the digital age.

Keywords: Personal data protection; Human rights; Brazilian General Data Protection Law (LGPD); Social rights; Digital society.

INTRODUÇÃO

A intensificação do uso de tecnologias digitais nas últimas décadas transformou profundamente as formas de interação social, econômica e institucional, consolidando a chamada sociedade digital. Nesse cenário, a coleta, o armazenamento e o compartilhamento de dados pessoais passaram a desempenhar papel central no funcionamento de serviços públicos e privados, influenciando diretamente a forma como os indivíduos acessam políticas públicas, exercem direitos e participam da vida social. A crescente dependência de sistemas informatizados e plataformas digitais trouxe benefícios relevantes em termos de eficiência administrativa e ampliação de serviços, mas também ampliou significativamente os riscos relacionados ao uso indevido de informações pessoais, expondo os indivíduos a situações de vulnerabilidade informacional e possíveis violações de direitos fundamentais (DONEDA, 2019).

Nesse contexto, a proteção de dados pessoais passou a ocupar posição estratégica no campo jurídico contemporâneo, deixando de ser tratada apenas como uma extensão do direito à privacidade para assumir dimensão própria no âmbito dos direitos humanos. O reconhecimento da proteção de dados como direito fundamental no ordenamento jurídico brasileiro, especialmente após a promulgação da Emenda Constitucional nº 115/2022, representou avanço normativo relevante ao inserir expressamente esse direito no rol constitucional, reafirmando sua vinculação à dignidade da pessoa humana e ao pleno exercício da cidadania (SARLET; MENDES, 2022). Paralelamente, a regulamentação do tratamento de dados pessoais pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) estabeleceu princípios e limites jurídicos voltados à proteção dos titulares de dados, criando parâmetros para o uso legítimo de informações pessoais em diferentes contextos sociais e institucionais (MENDES, 2020).

A relação entre proteção de dados pessoais e direitos humanos torna-se ainda mais evidente quando se observa que o tratamento de informações pessoais influencia diretamente a efetivação dos direitos sociais, tais como saúde, educação, assistência social e acesso a benefícios públicos. O uso intensivo de dados em políticas públicas pode favorecer a ampliação do acesso a serviços essenciais, mas também pode gerar riscos relacionados à discriminação, exclusão social e monitoramento excessivo de determinados grupos

populacionais (RODOTÀ, 2008). Assim, a utilização indiscriminada ou inadequada de dados pessoais pode comprometer direitos fundamentais, afetando não apenas a privacidade dos indivíduos, mas também a sua autonomia, liberdade e dignidade (MENDES; DONEDA, 2018).

Diante desse cenário, emerge um problema jurídico relevante que orienta o presente estudo: em que medida o uso crescente de dados pessoais por instituições públicas e privadas pode comprometer direitos humanos fundamentais, e quais são os limites jurídicos necessários para garantir a proteção da privacidade e da dignidade humana na efetivação dos direitos sociais? Tal questionamento evidencia a necessidade de refletir criticamente sobre os mecanismos normativos existentes e sobre os desafios decorrentes da utilização intensiva de informações pessoais em uma sociedade cada vez mais orientada por dados.

A justificativa para o desenvolvimento deste estudo fundamenta-se na crescente relevância social e jurídica da proteção de dados pessoais no contexto contemporâneo. O avanço tecnológico e a digitalização de serviços ampliaram significativamente a circulação de informações pessoais, tornando indispensável a definição de limites claros ao seu uso. A ausência de controle adequado ou o tratamento indevido dessas informações pode gerar consequências que ultrapassam a esfera individual, alcançando coletividades inteiras e comprometendo a efetivação de direitos sociais essenciais (SARLET, 2021). Nesse sentido, o debate sobre a proteção de dados pessoais não se restringe à dimensão tecnológica, mas envolve diretamente a garantia dos direitos humanos e a preservação dos princípios fundamentais que estruturam o Estado Democrático de Direito.

Nesse contexto, o presente estudo tem como objetivo geral analisar a proteção de dados pessoais como direito humano fundamental, identificando os limites jurídicos ao uso de informações pessoais e seus impactos na garantia dos direitos sociais e da dignidade humana. Para alcançar tal finalidade, foram definidos os seguintes objetivos específicos: examinar a evolução do direito à proteção de dados pessoais no âmbito dos direitos humanos; analisar os fundamentos constitucionais da proteção de dados pessoais no Brasil após a promulgação da Emenda Constitucional nº 115/2022; identificar os princípios e limites estabelecidos pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) quanto ao uso de informações pessoais; discutir os riscos decorrentes do uso excessivo ou inadequado de dados pessoais na efetivação dos direitos sociais; e refletir sobre a necessidade de equilíbrio entre inovação tecnológica, eficiência administrativa e proteção dos direitos humanos.

Quanto aos aspectos metodológicos, o estudo adota abordagem qualitativa, com base

em análise teórica e bibliográfica, fundamentada em doutrina jurídica especializada, legislação pertinente e produção científica relacionada ao tema da proteção de dados pessoais e dos direitos humanos. O método utilizado consiste na revisão crítica de literatura nacional e internacional, buscando identificar fundamentos normativos, princípios jurídicos e interpretações doutrinárias capazes de sustentar a análise proposta. A pesquisa assume caráter exploratório e descritivo, com o propósito de compreender os limites jurídicos ao uso de dados pessoais e suas implicações para a efetivação dos direitos sociais no contexto da sociedade digital (GIL, 2019).

Por fim, destaca-se que a análise proposta neste estudo busca contribuir para o aprofundamento do debate jurídico acerca da proteção de dados pessoais como direito humano fundamental, evidenciando a necessidade de construção de mecanismos normativos e institucionais capazes de assegurar o uso legítimo das informações pessoais, sem comprometer a dignidade humana e a efetividade dos direitos sociais na era digital.

2 A PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO HUMANO FUNDAMENTAL

A evolução tecnológica e a crescente digitalização das relações sociais trouxeram profundas transformações na forma como informações pessoais são coletadas, armazenadas e utilizadas. Nesse contexto, o direito à proteção de dados pessoais passou a assumir relevância central na tutela dos direitos humanos, especialmente diante dos riscos associados ao uso indevido de informações em ambientes digitais. Para compreender a atual configuração jurídica da proteção de dados pessoais como direito fundamental, torna-se necessário analisar a evolução histórica do direito à privacidade, bem como os fundamentos constitucionais que sustentam sua consolidação no ordenamento jurídico brasileiro.

Historicamente, o direito à privacidade surgiu como resposta às transformações sociais decorrentes do avanço tecnológico e da ampliação dos meios de comunicação. No final do século XIX, a crescente circulação de informações pessoais motivou o desenvolvimento de reflexões jurídicas voltadas à proteção da esfera privada dos indivíduos. Nesse período, consolidou-se a compreensão da privacidade como o direito de ser deixado em paz, conceito que posteriormente evoluiu para abranger a proteção contra interferências indevidas na vida pessoal e familiar (DONEDA, 2019). Com o avanço das tecnologias informacionais no século XX, especialmente com a disseminação de bancos de dados e sistemas informatizados, o direito à privacidade passou a incluir a proteção das informações pessoais como elemento

essencial da autonomia individual.

A partir da segunda metade do século XX, o crescimento do uso de tecnologias digitais e o aumento do fluxo de dados pessoais levaram ao reconhecimento da necessidade de regulamentação específica sobre o tratamento dessas informações. Nesse contexto, a proteção de dados pessoais deixou de ser compreendida apenas como extensão do direito à privacidade, passando a constituir um direito autônomo, dotado de características próprias e vinculado diretamente à dignidade da pessoa humana (MENDES, 2020). Essa evolução foi impulsionada pela constatação de que a manipulação indevida de dados pessoais pode gerar impactos significativos sobre a vida dos indivíduos, influenciando decisões relacionadas ao acesso a serviços, oportunidades sociais e garantias fundamentais.

No âmbito dos direitos humanos, a proteção de dados pessoais passou a ser compreendida como instrumento essencial para assegurar a autonomia e a liberdade dos indivíduos em sociedades marcadas pela intensa circulação de informações. Conforme observa RODOTÀ (2008), a sociedade contemporânea caracteriza-se por mecanismos constantes de monitoramento e vigilância, nos quais a coleta e o tratamento de dados podem gerar situações de controle social e limitação da liberdade individual. Nesse sentido, a proteção de dados pessoais constitui elemento indispensável para preservar a liberdade e evitar a utilização abusiva de informações capazes de comprometer direitos fundamentais.

No ordenamento jurídico brasileiro, o reconhecimento da proteção de dados pessoais como direito fundamental consolidou-se a partir da evolução normativa e constitucional ocorrida nas últimas décadas. A Constituição da República Federativa do Brasil de 1988 estabeleceu, desde sua promulgação, a proteção à intimidade, à vida privada, à honra e à imagem das pessoas, reconhecendo esses direitos como invioláveis e assegurando indenização pelo dano decorrente de sua violação. Embora o texto constitucional não tenha inicialmente previsto de forma expressa o direito à proteção de dados pessoais, sua interpretação sistemática permitiu reconhecer a proteção informacional como desdobramento dos direitos fundamentais relacionados à privacidade e à dignidade da pessoa humana (SARLET, 2021).

A consolidação definitiva desse reconhecimento ocorreu com a promulgação da Emenda Constitucional nº 115/2022, que incluiu expressamente a proteção de dados pessoais no rol dos direitos fundamentais previstos na Constituição brasileira. Tal alteração normativa representou marco jurídico relevante ao conferir maior segurança jurídica à tutela dos dados pessoais, reconhecendo sua centralidade na garantia da liberdade individual e da dignidade humana. Além disso, a inclusão desse direito no texto constitucional reforçou a necessidade

de criação de mecanismos eficazes de controle e fiscalização quanto ao tratamento de informações pessoais por instituições públicas e privadas.

A relação entre a proteção de dados pessoais e o princípio da dignidade da pessoa humana revela-se especialmente relevante no contexto contemporâneo. A dignidade humana constitui fundamento estruturante do Estado Democrático de Direito e orienta a interpretação e aplicação dos direitos fundamentais previstos na ordem constitucional. Nesse sentido, a proteção de dados pessoais representa instrumento essencial para assegurar que os indivíduos mantenham controle sobre suas informações, evitando situações de exposição indevida, discriminação ou exclusão social decorrentes do uso inadequado de dados pessoais (MENDES; DONEDA, 2018). A ausência de mecanismos adequados de proteção pode comprometer a autonomia individual e limitar a capacidade dos indivíduos de exercer plenamente seus direitos sociais.

Além da dignidade da pessoa humana, a proteção de dados pessoais apresenta relação direta com o direito à privacidade, reconhecido como um dos pilares fundamentais da proteção da esfera íntima dos indivíduos. O direito à privacidade envolve não apenas a proteção contra interferências indevidas na vida pessoal, mas também a garantia de controle sobre informações que dizem respeito ao indivíduo. Nesse contexto, a proteção de dados pessoais amplia o alcance da privacidade ao assegurar que o tratamento de informações pessoais ocorra de forma transparente, legítima e proporcional, evitando abusos e garantindo a preservação da autonomia informacional (DONEDA, 2019).

Outro aspecto relevante refere-se à relação entre a proteção de dados pessoais e a liberdade individual. Em sociedades baseadas na circulação massiva de informações, o uso inadequado de dados pode comprometer a liberdade dos indivíduos, especialmente quando informações pessoais são utilizadas para monitoramento, controle social ou tomada automatizada de decisões que impactam diretamente a vida dos cidadãos. Conforme destaca SARLET (2021), a proteção dos direitos fundamentais exige a adoção de mecanismos que assegurem a liberdade individual frente às novas formas de poder exercidas por meio da tecnologia e do tratamento de dados pessoais.

Nesse contexto, a proteção de dados pessoais deve ser compreendida como elemento essencial para garantir o equilíbrio entre inovação tecnológica e respeito aos direitos fundamentais. O reconhecimento constitucional desse direito não representa apenas avanço jurídico formal, mas também evidencia a necessidade de adaptação das estruturas normativas às transformações sociais decorrentes do desenvolvimento tecnológico. A crescente utilização

de dados pessoais em políticas públicas e serviços privados exige a definição de limites claros quanto ao seu tratamento, de modo a evitar violações de direitos humanos e assegurar a proteção da dignidade da pessoa humana.

Dessa forma, a proteção de dados pessoais consolida-se como direito humano fundamental indispensável à preservação da privacidade, da liberdade individual e da dignidade humana na sociedade contemporânea. A evolução histórica desse direito demonstra que sua consolidação normativa representa resposta necessária às novas formas de vulnerabilidade informacional decorrentes da sociedade digital. Assim, o reconhecimento constitucional da proteção de dados pessoais constitui instrumento fundamental para assegurar que o avanço tecnológico ocorra em consonância com os princípios fundamentais do Estado Democrático de Direito e com a efetivação dos direitos humanos.

2.1 LIMITES JURÍDICOS AO USO DE DADOS PESSOAIS NA LEGISLAÇÃO BRASILEIRA

A crescente utilização de dados pessoais em diferentes setores da sociedade impôs ao ordenamento jurídico brasileiro a necessidade de estabelecer parâmetros normativos claros para disciplinar o tratamento dessas informações. Nesse cenário, a promulgação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) representou marco regulatório essencial para a definição dos limites jurídicos ao uso de dados pessoais, estabelecendo princípios, conceitos e mecanismos de responsabilização voltados à proteção dos direitos fundamentais dos titulares de dados.

A legislação brasileira passou a reconhecer que o tratamento de dados pessoais não pode ocorrer de forma irrestrita, sendo necessário observar critérios jurídicos que assegurem a proteção da dignidade da pessoa humana, da privacidade e da liberdade individual. Nesse sentido, a referida legislação estabeleceu princípios fundamentais que orientam o uso legítimo de dados pessoais, definindo parâmetros que devem ser observados tanto por entidades públicas quanto privadas.

Entre os princípios estabelecidos pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), destaca-se o princípio da finalidade, segundo o qual o tratamento de dados pessoais deve ocorrer para propósitos legítimos, específicos e previamente informados ao titular. Esse princípio impede o uso indiscriminado de informações pessoais para finalidades distintas daquelas inicialmente comunicadas, evitando práticas abusivas e garantindo maior transparência nas atividades de tratamento de dados. Outro princípio relevante é o da

adequação, que determina que o tratamento deve ser compatível com as finalidades informadas ao titular, assegurando coerência entre a coleta e o uso das informações pessoais.

Além desses, o princípio da necessidade estabelece que o tratamento deve se limitar ao mínimo necessário para a realização de suas finalidades, evitando a coleta excessiva de dados pessoais. Esse princípio assume especial relevância diante do crescimento de práticas baseadas na coleta massiva de dados, muitas vezes sem justificativa proporcional. O princípio da transparência, por sua vez, exige que os titulares sejam informados de forma clara e acessível sobre o tratamento de seus dados, permitindo o exercício efetivo do controle informacional. Ainda nesse contexto, destacam-se os princípios da segurança e da prevenção, que impõem aos agentes de tratamento a adoção de medidas técnicas e administrativas capazes de evitar acessos não autorizados e situações de vazamento de dados pessoais (MENDES, 2020).

Outro elemento fundamental da legislação refere-se à definição dos conceitos de dados pessoais e dados pessoais sensíveis. Nos termos da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), dados pessoais são compreendidos como quaisquer informações relacionadas a pessoa natural identificada ou identificável, abrangendo desde dados básicos, como nome e endereço, até informações mais complexas relacionadas ao comportamento individual. Já os dados pessoais sensíveis são aqueles que dizem respeito à origem racial ou étnica, convicções religiosas, opiniões políticas, filiação sindical, dados referentes à saúde ou à vida sexual, bem como informações genéticas ou biométricas. A legislação confere tratamento diferenciado aos dados sensíveis em razão do elevado potencial de discriminação associado ao seu uso inadequado.

A distinção entre dados pessoais comuns e dados sensíveis revela preocupação do legislador com a proteção contra práticas discriminatórias e abusivas. O tratamento inadequado de dados sensíveis pode resultar em exclusão social, discriminação institucional e restrição indevida ao acesso a direitos fundamentais. Nesse sentido, a legislação estabelece requisitos mais rigorosos para o tratamento desses dados, exigindo maior nível de segurança e justificativa jurídica adequada para sua utilização (DONEDA, 2019).

Outro aspecto essencial para a definição dos limites jurídicos ao uso de dados pessoais refere-se às bases legais que autorizam o tratamento dessas informações. A legislação brasileira estabelece que o tratamento de dados pessoais somente pode ocorrer quando fundamentado em uma base legal válida, o que impede o uso arbitrário ou injustificado de informações pessoais. Entre as bases legais previstas na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), destaca-se o consentimento do titular, que consiste na

manifestação livre, informada e inequívoca pela qual o indivíduo autoriza o tratamento de seus dados para finalidade específica.

Contudo, é relevante observar que o consentimento não constitui a única base legal autorizadora do tratamento de dados pessoais. A legislação prevê outras hipóteses que legitimam o tratamento independentemente do consentimento, tais como o cumprimento de obrigação legal ou regulatória, a execução de políticas públicas, a realização de estudos por órgãos de pesquisa, a execução de contratos e a proteção da vida ou da incolumidade física do titular ou de terceiros. Essa multiplicidade de bases legais demonstra que a proteção de dados pessoais não se limita à autorização individual, mas envolve a necessidade de equilíbrio entre interesses coletivos e direitos individuais (MENDES; DONEDA, 2018).

Além das bases legais, a legislação brasileira estabelece mecanismos de responsabilização aplicáveis aos agentes de tratamento que utilizarem dados pessoais de forma indevida. A responsabilidade pelo uso inadequado de dados constitui elemento essencial para garantir a efetividade das normas de proteção e prevenir práticas abusivas. Nesse sentido, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) prevê que o controlador ou operador que causar dano patrimonial, moral, individual ou coletivo em decorrência de violação às normas de proteção de dados poderá ser responsabilizado civilmente.

A responsabilidade pelo uso indevido de dados pessoais apresenta caráter preventivo e reparatório, na medida em que incentiva a adoção de práticas seguras e estabelece sanções para situações de descumprimento das normas legais. Entre as sanções previstas na legislação, destacam-se advertências, multas administrativas, publicização da infração e bloqueio ou eliminação dos dados pessoais relacionados à irregularidade constatada. Tais medidas contribuem para fortalecer a cultura de proteção de dados e estimular a adoção de práticas responsáveis no tratamento de informações pessoais (SARLET, 2021).

Outro elemento relevante diz respeito à necessidade de implementação de mecanismos internos de governança e segurança da informação por parte das instituições que realizam tratamento de dados pessoais. A adoção de políticas internas, protocolos de segurança e sistemas de monitoramento constitui requisito indispensável para garantir a conformidade com os princípios estabelecidos pela legislação. A ausência de tais mecanismos pode resultar em vulnerabilidades capazes de comprometer a integridade e a confidencialidade das informações pessoais, ampliando os riscos de violação de direitos fundamentais.

Assim, observa-se que os limites jurídicos ao uso de dados pessoais estabelecidos pela legislação brasileira representam instrumento essencial para assegurar o tratamento

responsável e legítimo das informações pessoais. A definição de princípios orientadores, categorias de dados, bases legais e mecanismos de responsabilização demonstra preocupação do legislador em equilibrar o uso das tecnologias informacionais com a proteção dos direitos fundamentais. Tal equilíbrio revela-se indispensável para garantir que o avanço tecnológico ocorra de forma compatível com os valores constitucionais e com a preservação da dignidade da pessoa humana.

Dessa forma, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) consolida-se como instrumento jurídico essencial para delimitar o uso legítimo de dados pessoais no Brasil, estabelecendo parâmetros que visam prevenir abusos, responsabilizar condutas ilícitas e assegurar a proteção dos direitos fundamentais dos titulares de dados. A efetividade desses limites jurídicos depende não apenas da existência de normas legais, mas também da adoção de práticas institucionais responsáveis e da conscientização social quanto à importância da proteção de dados pessoais na sociedade contemporânea.

2.2 IMPACTOS DO USO DE DADOS PESSOAIS NA EFETIVAÇÃO DOS DIREITOS SOCIAIS

O uso intensivo de dados pessoais no contexto contemporâneo tem provocado profundas transformações na forma como os direitos sociais são planejados, executados e avaliados pelo Estado e por instituições privadas. A crescente digitalização das políticas públicas e dos serviços sociais possibilitou maior eficiência administrativa e ampliação do alcance de programas governamentais. Contudo, ao mesmo tempo em que o uso de dados pessoais contribui para a melhoria da gestão pública, também impõe desafios relevantes relacionados à proteção dos direitos fundamentais, especialmente no que se refere à privacidade, à dignidade humana e à igualdade no acesso a direitos sociais.

O uso de dados pessoais em políticas públicas representa uma das dimensões mais significativas da transformação digital no setor público. Informações pessoais são amplamente utilizadas para identificar beneficiários, planejar ações governamentais e monitorar a execução de programas sociais, permitindo maior precisão na distribuição de recursos e serviços. Entretanto, a utilização dessas informações exige rigoroso controle jurídico e institucional, uma vez que o tratamento inadequado de dados pode resultar em prejuízos coletivos e individuais. A ausência de critérios claros quanto ao uso dessas informações pode favorecer práticas discriminatórias, exclusão social e violação de direitos fundamentais, comprometendo a finalidade social das políticas públicas (MENDES, 2020).

Outro aspecto relevante refere-se ao fenômeno da vigilância digital, que se intensificou com a ampliação das tecnologias de monitoramento e coleta massiva de dados. Em sociedades altamente digitalizadas, a vigilância pode ocorrer de forma contínua e muitas vezes imperceptível aos indivíduos, gerando preocupação quanto ao uso abusivo de informações pessoais por instituições públicas e privadas. Conforme observa RODOTÀ (2008), a sociedade contemporânea caracteriza-se pela expansão de mecanismos de controle baseados em dados, que podem comprometer a liberdade individual e restringir o exercício pleno da cidadania. A vigilância excessiva, quando não devidamente regulamentada, pode transformar instrumentos de gestão pública em mecanismos de controle social incompatíveis com os princípios democráticos.

No âmbito das políticas públicas, destaca-se ainda o uso crescente de sistemas automatizados e algoritmos para análise e tomada de decisões. Esse cenário introduz o risco da discriminação algorítmica, fenômeno que ocorre quando sistemas automatizados reproduzem ou ampliam desigualdades sociais existentes. A utilização de algoritmos para selecionar beneficiários de programas sociais, por exemplo, pode gerar exclusão injustificada de determinados grupos populacionais, especialmente quando os dados utilizados para alimentar esses sistemas refletem desigualdades históricas e sociais. Nesse sentido, a ausência de transparência nos processos automatizados dificulta a identificação de falhas e limita a possibilidade de contestação por parte dos indivíduos afetados (DONEDA, 2019).

A discriminação algorítmica representa desafio significativo para a efetivação dos direitos sociais, pois pode comprometer o acesso igualitário a serviços essenciais. Quando decisões automatizadas são baseadas em critérios opacos ou inadequadamente validados, há risco de reforço de estigmas sociais e exclusão sistemática de indivíduos em situação de vulnerabilidade. Esse fenômeno evidencia a necessidade de mecanismos jurídicos capazes de assegurar transparência e controle sobre o uso de tecnologias automatizadas, evitando que a inovação tecnológica resulte em ampliação das desigualdades sociais (MENDES; DONEDA, 2018).

Outro fator que merece destaque refere-se à exclusão digital, entendida como a limitação de acesso a tecnologias digitais e serviços informatizados por parte de determinados grupos sociais. Embora a digitalização dos serviços públicos tenha ampliado a disponibilidade de políticas sociais, também criou barreiras para indivíduos que não possuem acesso adequado à internet ou habilidades tecnológicas suficientes para utilizar sistemas digitais. Essa realidade demonstra que a adoção indiscriminada de tecnologias digitais pode resultar

em acesso desigual a direitos sociais, especialmente entre populações economicamente vulneráveis (SARLET, 2021).

A exclusão digital revela-se particularmente problemática em contextos nos quais o acesso a serviços essenciais depende exclusivamente de plataformas digitais. Nesses casos, indivíduos sem acesso à tecnologia ou com baixa alfabetização digital, podem enfrentar dificuldades significativas para exercer seus direitos, o que compromete o princípio da igualdade e limita a efetividade das políticas públicas. Assim, a implementação de soluções digitais deve considerar a diversidade social e garantir mecanismos alternativos de acesso aos serviços públicos, evitando a marginalização de grupos vulneráveis.

Além dos riscos relacionados à vigilância e à exclusão digital, o uso inadequado de dados pessoais também apresenta impactos diretos sobre a dignidade da pessoa humana. A exposição indevida de informações pessoais pode gerar danos morais, sociais e econômicos, afetando a reputação e a autonomia dos indivíduos. A utilização de dados pessoais sem consentimento ou em desacordo com as finalidades previamente estabelecidas constitui violação dos direitos fundamentais, podendo comprometer a integridade da esfera privada e a liberdade individual. Nesse sentido, a proteção da dignidade humana exige que o tratamento de dados pessoais ocorra de forma responsável e proporcional, respeitando os limites jurídicos estabelecidos pela legislação (MENDES, 2020).

Outro impacto relevante refere-se ao acesso desigual a direitos sociais decorrente do uso inadequado de dados pessoais. A utilização de informações para definir prioridades ou restringir o acesso a determinados serviços pode resultar em práticas discriminatórias e injustificáveis. Em contextos de escassez de recursos, o uso de dados para selecionar beneficiários deve observar critérios transparentes e juridicamente fundamentados, evitando a exclusão arbitrária de indivíduos ou grupos sociais. A ausência de mecanismos de controle e supervisão pode favorecer decisões baseadas em critérios inadequados, comprometendo a legitimidade das políticas públicas e violando direitos fundamentais.

Nesse cenário, torna-se evidente que o uso de dados pessoais apresenta potencial tanto para promover quanto para limitar a efetivação dos direitos sociais. Quando utilizado de forma responsável, o tratamento de dados pode contribuir para a melhoria da eficiência administrativa e para a ampliação do acesso a serviços essenciais. Contudo, quando utilizado de forma inadequada, pode gerar desigualdades, exclusão social e violação de direitos fundamentais, evidenciando a necessidade de equilíbrio entre inovação tecnológica e proteção dos direitos humanos.

A análise dos impactos do uso de dados pessoais na efetivação dos direitos sociais demonstra que a proteção de dados não constitui apenas questão técnica ou administrativa, mas elemento central para a preservação dos valores democráticos e para a garantia da justiça social. A definição de limites jurídicos claros e a implementação de mecanismos de controle efetivos são indispensáveis para assegurar que o uso de tecnologias informacionais contribua para a promoção dos direitos sociais, sem comprometer a dignidade humana e a igualdade entre os indivíduos.

Dessa forma, o tratamento de dados pessoais deve ser orientado por princípios éticos e jurídicos capazes de garantir o respeito aos direitos fundamentais e a proteção das populações mais vulneráveis. A efetivação dos direitos sociais na era digital depende da construção de modelos de governança que conciliem eficiência tecnológica com responsabilidade social, evitando que o avanço tecnológico resulte em novas formas de exclusão e desigualdade. Nesse sentido, a análise crítica dos impactos do uso de dados pessoais constitui etapa essencial para compreender os desafios contemporâneos relacionados à proteção dos direitos humanos e à consolidação de uma sociedade digital mais justa e inclusiva.

2.3 O EQUILÍBRIO ENTRE INOVAÇÃO TECNOLÓGICA E PROTEÇÃO DOS DIREITOS HUMANOS

O avanço tecnológico verificado nas últimas décadas consolidou novas formas de produção, armazenamento e utilização de dados pessoais, criando oportunidades significativas para o desenvolvimento econômico e social. Contudo, a expansão dessas tecnologias também introduziu riscos relacionados à proteção dos direitos fundamentais, exigindo a construção de mecanismos jurídicos capazes de equilibrar inovação tecnológica e proteção dos direitos humanos. Nesse contexto, torna-se indispensável a definição de estratégias regulatórias que assegurem o uso legítimo das tecnologias informacionais, sem comprometer valores essenciais como a dignidade humana, a privacidade e a liberdade individual.

A necessidade de regulação adequada constitui elemento central para garantir que o desenvolvimento tecnológico ocorra de forma compatível com os princípios do Estado Democrático de Direito. O tratamento massivo de dados pessoais, aliado à crescente automação de decisões, ampliou a capacidade de monitoramento e controle sobre os indivíduos, tornando imprescindível a atuação normativa do Estado para prevenir abusos e assegurar a proteção dos titulares de dados. Nesse sentido, a existência de instrumentos jurídicos específicos, como a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018),

representa avanço significativo ao estabelecer parâmetros legais para o tratamento de dados pessoais e definir responsabilidades aplicáveis aos agentes envolvidos.

Entretanto, a mera existência de normas jurídicas não garante, por si só, a efetiva proteção dos direitos fundamentais. A regulação tecnológica exige constante atualização normativa, uma vez que os avanços tecnológicos ocorrem em ritmo acelerado e frequentemente superam a capacidade de resposta do legislador. Dessa forma, a construção de modelos regulatórios eficientes deve considerar a flexibilidade normativa e a adoção de princípios jurídicos capazes de orientar decisões em contextos tecnológicos complexos. A regulação inadequada ou insuficiente pode favorecer práticas abusivas, comprometendo a confiança social nas instituições e ampliando situações de vulnerabilidade informacional (MENDES, 2020).

Outro aspecto fundamental refere-se à definição de limites éticos ao uso de dados pessoais. O desenvolvimento tecnológico ampliou significativamente a capacidade de coleta e análise de informações pessoais, permitindo a construção de perfis detalhados sobre comportamentos individuais. Embora tais recursos possam contribuir para a melhoria de serviços e políticas públicas, também apresentam riscos relacionados ao uso indevido de dados e à manipulação de informações pessoais. Nesse contexto, a ética no tratamento de dados assume papel central na definição de práticas responsáveis e transparentes, evitando que interesses econômicos ou institucionais se sobreponham à proteção dos direitos humanos (RODOTÀ, 2008).

A definição de limites éticos torna-se especialmente relevante diante da utilização crescente de tecnologias baseadas em inteligência artificial e algoritmos decisórios. Esses sistemas possuem capacidade de influenciar decisões que afetam diretamente a vida dos indivíduos, como concessão de benefícios sociais, acesso a crédito ou seleção para serviços públicos. A ausência de critérios éticos claros pode resultar em decisões automatizadas injustas ou discriminatórias, comprometendo a igualdade e a dignidade humana. Assim, a incorporação de princípios éticos no desenvolvimento tecnológico constitui requisito indispensável para assegurar que a inovação ocorra de forma socialmente responsável (DONEDA, 2019).

A proteção contra abusos no tratamento de dados pessoais também depende da implementação de mecanismos eficazes de controle e fiscalização. A crescente complexidade dos sistemas digitais exige a adoção de estratégias preventivas capazes de identificar vulnerabilidades e reduzir riscos de vazamentos ou acessos indevidos. Nesse sentido, a adoção

de medidas técnicas e administrativas adequadas representa elemento essencial para garantir a integridade e a confidencialidade das informações pessoais. A ausência de tais medidas pode resultar em danos significativos aos indivíduos e comprometer a credibilidade das instituições responsáveis pelo tratamento de dados (MENDES; DONEDA, 2018).

Outro elemento central para o equilíbrio entre inovação tecnológica e proteção dos direitos humanos refere-se à governança de dados. A governança consiste na implementação de políticas, procedimentos e estruturas organizacionais voltadas à gestão responsável das informações pessoais. Esse modelo envolve a definição de responsabilidades internas, a adoção de padrões de segurança e a realização de avaliações periódicas sobre os riscos associados ao tratamento de dados. A governança adequada permite identificar falhas operacionais e promover ajustes necessários para garantir a conformidade com as normas legais e os princípios éticos aplicáveis (SARLET, 2021).

A governança de dados também contribui para fortalecer a transparência institucional, permitindo que os titulares compreendam como suas informações são utilizadas e quais medidas são adotadas para protegê-las. A transparência constitui elemento essencial para a construção da confiança social, especialmente em contextos nos quais o uso de dados pessoais é intensivo. A ausência de transparência pode gerar insegurança jurídica e favorecer práticas incompatíveis com os direitos fundamentais, comprometendo a legitimidade das instituições responsáveis pelo tratamento de dados.

Além da governança, a responsabilização institucional constitui mecanismo indispensável para assegurar o cumprimento das normas de proteção de dados pessoais. A responsabilização envolve a aplicação de sanções administrativas, civis e eventualmente penais aos agentes que utilizarem dados pessoais em desacordo com a legislação vigente. Esse mecanismo possui caráter preventivo e educativo, incentivando a adoção de práticas responsáveis e desencorajando condutas ilícitas. A efetividade das normas jurídicas depende, em grande medida, da existência de sistemas de responsabilização capazes de identificar infrações e aplicar penalidades proporcionais à gravidade das condutas (MENDES, 2020).

A responsabilização institucional também contribui para fortalecer a cultura de proteção de dados nas organizações públicas e privadas. A adoção de práticas responsáveis no tratamento de dados pessoais deve ser compreendida não apenas como obrigação legal, mas como compromisso institucional com a proteção dos direitos humanos. Nesse sentido, a implementação de programas de conformidade e treinamento contínuo dos agentes envolvidos no tratamento de dados constitui medida relevante para prevenir violações e garantir a

observância das normas legais.

A análise do equilíbrio entre inovação tecnológica e proteção dos direitos humanos evidencia que o desenvolvimento tecnológico não pode ocorrer de forma dissociada dos princípios fundamentais que estruturam a ordem jurídica. A incorporação de tecnologias digitais nos diferentes setores da sociedade deve ser orientada por critérios jurídicos e éticos capazes de assegurar o respeito à dignidade humana e à liberdade individual. O desafio contemporâneo consiste em construir modelos regulatórios que permitam a utilização eficiente das tecnologias informacionais, sem comprometer a proteção dos direitos fundamentais.

Nesse contexto, a busca pelo equilíbrio entre inovação e proteção de direitos exige atuação conjunta do Estado, das instituições privadas e da sociedade civil. A construção de um ambiente digital seguro depende da cooperação entre diferentes atores sociais e da adoção de práticas responsáveis no tratamento de dados pessoais. A ausência de integração entre esses elementos pode resultar em lacunas regulatórias e fragilizar a proteção dos direitos humanos em ambientes digitais.

Dessa forma, o equilíbrio entre inovação tecnológica e proteção dos direitos humanos representa desafio contínuo e dinâmico, que exige atualização constante das estruturas normativas e institucionais.

CONSIDERAÇÕES FINAIS

O presente estudo teve como objetivo analisar a proteção de dados pessoais como direito humano fundamental, identificando os limites jurídicos ao uso de informações pessoais e seus impactos na garantia dos direitos sociais e da dignidade humana no contexto da sociedade digital. A investigação partiu da compreensão de que a crescente digitalização das relações sociais e institucionais ampliou significativamente o uso de dados pessoais, tornando indispensável a construção de mecanismos jurídicos capazes de assegurar o tratamento responsável dessas informações.

Em resposta ao problema de pesquisa proposto — que buscou compreender em que medida o uso crescente de dados pessoais por instituições públicas e privadas pode comprometer direitos humanos fundamentais e quais são os limites jurídicos necessários para garantir a proteção da privacidade e da dignidade humana na efetivação dos direitos sociais — verificou-se que o uso inadequado ou excessivo de dados pessoais representa risco concreto à proteção dos direitos fundamentais. A análise desenvolvida ao longo do estudo evidenciou que

a utilização indiscriminada de dados pode gerar situações de exclusão social, discriminação algorítmica, vigilância excessiva e acesso desigual a políticas públicas, comprometendo a efetividade dos direitos sociais e a autonomia individual.

A síntese dos resultados obtidos demonstra que a consolidação da proteção de dados pessoais como direito fundamental representa avanço significativo no ordenamento jurídico brasileiro, especialmente após a promulgação da Emenda Constitucional nº 115/2022, que reconheceu expressamente a proteção de dados pessoais como direito fundamental. Esse reconhecimento fortaleceu a proteção jurídica da privacidade e reafirmou a necessidade de adoção de mecanismos normativos eficazes para disciplinar o tratamento de informações pessoais. Nesse sentido, a regulamentação estabelecida pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) consolidou princípios, bases legais e instrumentos de responsabilização capazes de delimitar o uso legítimo de dados pessoais, estabelecendo parâmetros essenciais para a proteção dos titulares de dados.

A análise dos capítulos desenvolvidos permitiu identificar que os limites jurídicos ao uso de dados pessoais não se restringem ao cumprimento formal da legislação, mas exigem a incorporação de práticas institucionais responsáveis e mecanismos de governança adequados. Observou-se que a adoção de políticas internas de segurança da informação, a implementação de protocolos de transparência e a criação de sistemas de responsabilização institucional constituem medidas indispensáveis para prevenir abusos e assegurar a conformidade com os princípios legais. A ausência dessas medidas pode comprometer a eficácia das normas existentes, ampliando riscos relacionados ao uso indevido de informações pessoais. A reflexão crítica decorrente da análise realizada evidencia que o avanço tecnológico, embora represente oportunidade para a ampliação do acesso a direitos sociais, também pode aprofundar desigualdades estruturais quando não acompanhado de mecanismos eficazes de proteção jurídica. A utilização de tecnologias digitais em políticas públicas, quando orientada por critérios inadequados ou pouco transparentes, pode reforçar práticas discriminatórias e limitar o acesso igualitário a serviços essenciais. Assim, a proteção de dados pessoais deve ser compreendida como elemento essencial para a promoção da justiça social e para a garantia da igualdade material entre os indivíduos.

Outro aspecto relevante identificado ao longo do estudo refere-se à necessidade de equilíbrio entre inovação tecnológica e proteção dos direitos humanos. A análise demonstrou que o desenvolvimento tecnológico não deve ser compreendido como fenômeno neutro, mas como processo que envolve escolhas institucionais e decisões normativas capazes de impactar

diretamente a vida dos cidadãos. A ausência de controle adequado sobre o uso de dados pessoais pode transformar instrumentos tecnológicos em mecanismos de vigilância e exclusão, comprometendo valores fundamentais do Estado Democrático de Direito.

No que se refere aos possíveis caminhos futuros, destaca-se a necessidade de fortalecimento contínuo das estruturas regulatórias e institucionais voltadas à proteção de dados pessoais. A rápida evolução das tecnologias digitais exige atualização constante das normas jurídicas e a ampliação da capacidade institucional de fiscalização e controle. Nesse sentido, torna-se fundamental investir em políticas públicas voltadas à educação digital e à conscientização social sobre os direitos relacionados à proteção de dados pessoais, permitindo que os indivíduos exerçam de forma efetiva o controle sobre suas informações.

Além disso, evidencia-se a importância do desenvolvimento de modelos de governança de dados que priorizem a transparência, a responsabilidade institucional e a participação social nos processos decisórios relacionados ao tratamento de informações pessoais. A incorporação de critérios éticos no desenvolvimento tecnológico constitui elemento essencial para prevenir abusos e assegurar que a inovação ocorra de forma compatível com os princípios fundamentais da dignidade humana e da liberdade individual.

Por fim, conclui-se que a proteção de dados pessoais representa instrumento indispensável para a efetivação dos direitos sociais na sociedade digital, exigindo atuação integrada entre Estado, instituições privadas e sociedade civil. A consolidação de mecanismos jurídicos eficazes, aliada à adoção de práticas institucionais responsáveis, constitui condição essencial para assegurar que o avanço tecnológico contribua para a promoção dos direitos humanos e para a construção de uma sociedade mais justa, inclusiva e orientada pela proteção da dignidade humana.

REFERÊNCIAS

BRASIL. **Lei Geral de Proteção de Dados Pessoais** (Lei nº 13.709/2018).

BRASIL. **Emenda Constitucional nº 115/2022**.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 7. ed. São Paulo: Atlas, 2019.

MENDES, Laura Schertel. **Proteção de dados pessoais**: fundamento, conceitos e modelo de aplicação. São Paulo: Thomson Reuters Brasil, 2020.

MENDES, Laura Schertel; DONEDA, Danilo. **Comentário à Lei Geral de Proteção de Dados**. São Paulo: Revista dos Tribunais, 2018.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. 13. ed. Porto Alegre: Livraria do Advogado, 2021.

SARLET, Ingo Wolfgang; MENDES, Gilmar Ferreira. **Curso de Direito Constitucional**. 13. ed. São Paulo: Saraiva, 2022.