REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

A DIGNIDADE DA PESSOA HUMANA COMO FUNDAMENTO DA PROTEÇÃO DE DADOS PESSOAIS SENSÍVEIS NO AMBIENTE DIGITAL

HUMAN DIGNITY AS A FOUNDATION FOR THE PROTECTION OF SENSITIVE PERSONAL DATA IN THE DIGITAL ENVIRONMENT

Ciências Sociais Aplicadas • 01/11/2026

REGISTRO DOI: 10.70773/revistatopicos/793412969

Amábilie Carolline Santos Sampaio[1]

Francisco Lopes Fernandes Netto[2]

RESUMO

A transformação digital ampliou a capacidade de coleta, correlação e utilização de informações relacionadas aos indivíduos, atribuindo aos dados pessoais sensíveis relevância crescente na tutela dos direitos fundamentais. O presente artigo analisa a proteção desses dados no ambiente digital à luz do princípio da dignidade da pessoa humana, examinando o regime jurídico da Lei Geral de Proteção de Dados Pessoais, os riscos de perfilamento e discriminação algorítmica e os mecanismos de prevenção, governança e responsabilização. A pesquisa é básica, qualitativa, exploratória e descritiva, orientada pelo método dedutivo e desenvolvida mediante pesquisa bibliográfica e documental em legislação, artigos científicos, dissertações, teses e documentos institucionais. Verifica-se que a proteção dos dados sensíveis não se esgota no sigilo ou no consentimento, exigindo interpretação material dos princípios da finalidade, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização. Conclui-se que a dignidade humana atua como fundamento interpretativo e limite material ao tratamento de dados, impondo que inovação tecnológica, decisões automatizadas e formação de perfis permaneçam subordinadas à autonomia, à igualdade e ao livre desenvolvimento da personalidade.

Palavras-chave: dados pessoais sensíveis; dignidade da pessoa humana; LGPD; discriminação algorítmica; direitos fundamentais.

ABSTRACT

Digital transformation has expanded the capacity to collect, correlate and use information related to individuals, giving sensitive personal data increasing relevance in the protection of fundamental rights. This article analyzes the protection of such data in the digital environment in light of the principle of human dignity, examining

the Brazilian General Data Protection Law, the risks of profiling and algorithmic discrimination, and mechanisms of prevention, governance and accountability. The research is basic, qualitative, exploratory and descriptive, guided by the deductive method and developed through bibliographic and documentary research. The study finds that protection of sensitive data cannot be reduced to secrecy or consent and requires a substantive application of purpose limitation, necessity, transparency, security, prevention, non-discrimination and accountability. It concludes that human dignity operates both as an interpretive foundation and as a material limit on data processing.
Keywords: sensitive personal data; human dignity; LGPD; algorithmic discrimination; fundamental rights.

1. INTRODUÇÃO

A expansão das tecnologias digitais intensificou a coleta, o armazenamento, o compartilhamento e o tratamento de informações pessoais, fazendo com que a proteção de dados assumisse especial relevância no Direito contemporâneo. Nesse cenário, a tutela jurídica torna-se ainda mais necessária quando envolve dados pessoais sensíveis, pois essas informações alcançam aspectos particulares da identidade do indivíduo e podem, quando utilizadas de maneira indevida, ocasionar exposição e práticas discriminatórias.

No ordenamento jurídico brasileiro, a proteção de dados pessoais foi expressamente reconhecida como direito fundamental pela Emenda Constitucional nº 115/2022, que acrescentou o inciso LXXIX ao art. 5º da Constituição Federal. O dispositivo estabelece que “é assegurado, nos termos da lei, o direito à proteção dos dados

pessoais, inclusive nos meios digitais" (Brasil, 1988, art. 5º, LXXIX). Desse modo, a proteção de dados passou a integrar expressamente o conjunto de direitos e garantias fundamentais, reforçando a tutela constitucional da pessoa também no ambiente digital.

A construção da legislação brasileira sobre proteção de dados pessoais recebeu influência do Regulamento Geral sobre a Proteção de Dados (RGPD), também conhecido pela sigla inglesa GDPR, instituído pelo Regulamento (UE) 2016/679, de 27 de abril de 2016, e aplicável desde 25 de maio de 2018. A norma europeia estabelece regras para o tratamento de dados pessoais e assegura direitos aos seus titulares, orientando-se por princípios como transparência, limitação das finalidades e minimização dos dados, além de exigir medidas de segurança e responsabilização dos agentes de tratamento (União Europeia, 2016, arts. 5º e 32).

Nesse sentido, o regulamento constituiu uma importante referência para a elaboração da LGPD, contribuindo para a adoção, no Brasil, de um modelo de proteção centrado nos direitos dos titulares e nos deveres daqueles que tratam suas informações pessoais.

Essa proteção relaciona-se ao princípio da dignidade da pessoa humana, previsto no art. 1º, inciso III, da Constituição Federal como fundamento da República Federativa do Brasil (Brasil, 1988). No campo infraconstitucional, a Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), regulamenta o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018, art. 1º).

A LGPD atribui proteção específica aos dados pessoais sensíveis, definidos no art. 5º, inciso II, como aqueles relacionados à origem racial ou étnica, convicção religiosa, opinião política, filiação sindical ou a organização de caráter religioso, filosófico ou político, saúde, vida sexual, bem como dados genéticos ou biométricos vinculados a uma pessoa natural (Brasil, 2018). Além disso, o art. 11 da Lei nº 13.709/2018 estabelece hipóteses específicas para o tratamento desses dados, entre elas o consentimento específico e destacado do titular para finalidades determinadas e as demais situações legais em que o tratamento é admitido sem consentimento (Brasil, 2018, art. 11, I e II).

Apesar do avanço normativo, o tratamento de dados pessoais sensíveis no ambiente digital permanece relacionado a riscos como acesso não autorizado, vazamento, exposição e compartilhamento indevido de informações. Tais ocorrências podem repercutir sobre direitos da personalidade e produzir consequências sociais e discriminatórias, evidenciando a necessidade de examinar a proteção desses dados a partir dos fundamentos constitucionais que tutelam a pessoa humana e dos princípios da segurança, prevenção e não discriminação estabelecidos pela Lei Geral de Proteção de Dados Pessoais (Brasil, 2018, art. 6º, VII, VIII e IX).

Diante desse contexto, a pesquisa foi orientada pelo seguinte problema: de que forma o princípio da dignidade da pessoa humana fundamenta a proteção dos dados pessoais sensíveis no ambiente digital, e quais mecanismos jurídicos se mostram aptos a assegurar essa proteção de maneira efetiva?

O objetivo geral consistiu em analisar a proteção de dados pessoais sensíveis no ambiente digital à luz do princípio da dignidade da

pessoa humana. Especificamente, buscou-se examinar o conteúdo jurídico da dignidade da pessoa humana como fundamento constitucional da tutela da personalidade; estudar os dados pessoais sensíveis e sua relevância jurídica; analisar os mecanismos de proteção previstos na LGPD; verificar a efetividade desses mecanismos no ambiente digital; e identificar os principais desafios jurídicos relacionados à proteção desses dados.

A pesquisa justificou-se pela crescente circulação e utilização de informações pessoais no ambiente digital e pela especial vulnerabilidade relacionada ao tratamento de dados sensíveis. Sua relevância jurídica e social decorre da necessidade de compreender em que medida os instrumentos estabelecidos pelo ordenamento brasileiro são capazes de preservar a privacidade, a liberdade, a não discriminação e o livre desenvolvimento da personalidade diante das transformações tecnológicas contemporâneas.

Metodologicamente, foi desenvolvida pesquisa de natureza básica, com abordagem qualitativa e objetivos exploratórios e descritivos, orientada pelo método dedutivo. Quanto aos procedimentos, realizou-se pesquisa bibliográfica e documental, mediante análise de livros, artigos científicos, trabalhos acadêmicos, legislação e documentos jurídicos relacionados à dignidade da pessoa humana, aos dados pessoais sensíveis, à privacidade e à proteção de dados. O levantamento contemplou materiais disponíveis na SciELO, LexML Brasil e Biblioteca do Supremo Tribunal Federal, selecionados conforme sua pertinência e contribuição para o problema investigado.

2. A DIGNIDADE DA PESSOA HUMANA COMO FUNDAMENTO DA TUTELA DA PERSONALIDADE

A tutela dos direitos da personalidade passou a ser compreendida, no Direito contemporâneo, a partir de uma perspectiva mais ampla, voltada à proteção da pessoa em sua integralidade. Essa construção permite que novos riscos à autonomia, à identidade e à liberdade sejam juridicamente enfrentados mesmo quando não correspondam, de maneira exata, às formas tradicionais de violação dos direitos da personalidade. Zanini e Queiroz (2023) situam a dignidade da pessoa humana como cláusula geral dessa tutela, conferindo ao sistema jurídico capacidade de acompanhar as transformações sociais sem restringir a proteção da pessoa a um conjunto fechado de situações previamente tipificadas.

Essa leitura ganha novos contornos na sociedade de dados. A crescente mediação tecnológica das relações sociais permite que comportamentos, preferências e características individuais sejam registrados e submetidos a operações capazes de produzir conhecimento sobre as pessoas. Melo e Alvim (2023) destacam que recursos como *big data* e inteligência artificial ampliaram a capacidade de utilização de informações e, paralelamente, fizeram surgir novos desafios à preservação da dignidade humana. A questão jurídica deixa, assim, de envolver apenas aquilo que alguém pretende manter em segredo e passa a alcançar os efeitos que o processamento de informações pode produzir sobre sua vida.

Nesse cenário, ganha relevância a chamada dimensão informacional da personalidade. Dados aparentemente dispersos podem ser reunidos, correlacionados e utilizados para formar perfis, estabelecer classificações ou orientar decisões a respeito de determinado indivíduo. Yaegashi, Otero e Maia (2024) relacionam a proteção de dados à tutela da personalidade justamente porque a utilização das informações pessoais pode repercutir sobre a autonomia privada e

sobre a forma como o sujeito é reconhecido e tratado socialmente. A informação, portanto, não interessa ao Direito apenas por seu conteúdo, mas também pelos efeitos que seu tratamento pode produzir sobre a pessoa à qual se refere.

Essa mudança evidencia a insuficiência de uma concepção de privacidade limitada ao sigilo. Almeida (2023) observa que a ideia tradicional de privacidade, associada principalmente ao isolamento ou à não divulgação de informações, não responde integralmente às formas contemporâneas de tratamento de dados. Uma informação pode ter sido obtida de maneira legítima e, posteriormente, ser combinada ou empregada em finalidade capaz de afetar seu titular. A proteção jurídica precisa alcançar, por isso, o percurso da informação e os usos que dela podem decorrer.

É nesse ponto que a autodeterminação informativa assume especial importância. O instituto desloca a discussão da simples ocultação de informações para a possibilidade de o indivíduo exercer direitos diante de sua utilização. Carmo (2024) vincula a autodeterminação informativa à dignidade da pessoa humana, destacando sua importância para a preservação dos direitos individuais no contexto digital. Não se trata, portanto, de atribuir ao titular controle absoluto sobre qualquer operação envolvendo seus dados, mas de reconhecer que ele não pode ser colocado em posição de completa passividade diante de processos informacionais capazes de repercutir sobre sua esfera pessoal.

Essa concepção mostra-se especialmente relevante em relações marcadas por assimetria informacional e elevada complexidade tecnológica. Muitas operações são realizadas por sistemas cujo funcionamento e consequências não são imediatamente

perceptíveis pelo titular. A liberdade individual, nesse ambiente, pressupõe condições jurídicas que assegurem transparência, conhecimento e possibilidades efetivas de atuação diante do tratamento de informações, afastando a ideia de que a proteção da personalidade dependa exclusivamente de uma reação posterior à ocorrência do dano.

A formação de perfis constitui exemplo expressivo dessa mudança. O processamento de diferentes informações pode resultar em inferências sobre hábitos, interesses ou características de uma pessoa, ainda que essas conclusões não tenham sido diretamente fornecidas por ela. Yaegashi, Otero e Maia (2024) sustentam que a proteção de dados assume contornos próprios exatamente porque as tecnologias informacionais criaram novas possibilidades de interferência sobre a personalidade. Nesse contexto, o risco jurídico pode decorrer não apenas da exposição pública de uma informação, mas também da maneira pela qual ela é interpretada e empregada em processos de classificação e decisão.

Sob essa perspectiva, a dignidade humana funciona como limite à instrumentalização da pessoa pela tecnologia. O indivíduo não pode ser reduzido a um conjunto de informações destinado exclusivamente à exploração econômica, à categorização ou à tomada automatizada de decisões. Melo e Alvim (2023) ressaltam que o desenvolvimento tecnológico deve ser compatibilizado com a preservação da pessoa, sobretudo diante da ampliação da capacidade de processamento de dados e da incorporação dessas tecnologias em diferentes esferas da vida social.

Assim, a proteção da personalidade no ambiente digital não corresponde à criação de uma nova categoria de dignidade, mas à

aplicação de sua função protetiva a formas contemporâneas de interferência sobre a pessoa. Autonomia, identidade e livre desenvolvimento da personalidade passam a ser examinados também a partir da circulação e do uso das informações que representam o indivíduo em ambientes digitais. A tutela jurídica dos dados revela-se, nesse sentido, uma projeção da proteção da própria pessoa diante das transformações tecnológicas.

Essa construção fornece a base para compreender por que determinadas informações exigem cautelas jurídicas mais intensas. Quando os dados demonstram características particularmente vinculadas à identidade ou à esfera existencial do titular, sua utilização pode ampliar riscos de exposição, classificação e discriminação. É a partir dessa premissa que se torna possível avançar para o estudo dos dados pessoais sensíveis e de sua posição específica no sistema de proteção de dados.

3. DADOS PESSOAIS SENSÍVEIS E A PROTEÇÃO JURÍDICA DIFERENCIADA NA LGPD

A distinção entre dados pessoais comuns e dados pessoais sensíveis não representa mera classificação terminológica. Ela traduz uma escolha legislativa fundada na percepção de que determinadas informações possuem maior capacidade de interferir na esfera existencial do indivíduo e de produzir consequências discriminatórias. Por isso, a tutela reforçada dos dados sensíveis deve ser compreendida como mecanismo de proteção da igualdade, da autonomia e do livre desenvolvimento da personalidade, e não apenas como técnica de preservação do sigilo.

Nos termos do art. 5º, II, da Lei nº 13.709/2018, são sensíveis os dados referentes à origem racial ou étnica, convicção religiosa, opinião política, filiação sindical ou a organização de caráter religioso, filosófico ou político, saúde, vida sexual e dados genéticos ou biométricos vinculados a pessoa natural (Brasil, 2018). A Autoridade Nacional de Proteção de Dados esclarece que tais informações recebem proteção mais intensa por se relacionarem a aspectos especialmente íntimos da personalidade (ANPD, 2026).

A especialidade do regime jurídico decorre do potencial de utilização da informação para diferenciar pessoas em contextos nos quais a diferenciação pode se converter em exclusão. O conhecimento de uma característica racial, religiosa, biométrica, genética ou relacionada à saúde pode interferir em decisões sobre emprego, crédito, seguro, acesso a serviços e oportunidades. A lesividade do tratamento não depende, assim, apenas da exposição pública do dado, mas também da finalidade para a qual ele é empregado e dos efeitos produzidos sobre o titular.

Costa (2024), ao investigar dados sensíveis relacionados à vida sexual sob a perspectiva do Direito Antidiscriminatório, demonstra que a proteção informacional precisa dialogar com a igualdade material e com os impactos do tratamento massivo de dados sobre grupos vulnerabilizados. Essa perspectiva desloca a discussão do simples controle individual da informação para a análise das estruturas capazes de produzir desvantagens coletivas a partir de classificações informacionais.

A delimitação legislativa da categoria suscita problema relevante. Gimenez (2025) questiona se o rol previsto no art. 5º, II, deve ser compreendido como taxativo ou se a evolução tecnológica exige

interpretação capaz de abranger informações que, embora não nominadas expressamente pela lei, apresentem potencial equivalente de discriminação. A autora sustenta que a rigidez classificatória pode se mostrar insuficiente diante de tecnologias capazes de produzir novas informações mediante inferências e correlações.

A questão pode ser percebida quando uma plataforma não coleta diretamente a religião ou a condição de saúde de um usuário, mas combina localização, histórico de pesquisas, páginas acessadas, hábitos de consumo e padrões de deslocamento para inferir essas características. Nesse caso, a informação sensível não foi necessariamente fornecida pelo titular: foi produzida pelo próprio tratamento. Uma interpretação estritamente literal poderia proteger o dado declarado e deixar em zona de menor proteção o atributo inferido, embora ambos possam gerar consequências semelhantes.

Cezarino (2024) oferece exemplo concreto da insuficiência potencial das categorias positivadas ao examinar a ausência expressa da identidade de gênero no rol de dados sensíveis da LGPD. A autora relaciona essa ausência a um problema de reconhecimento jurídico, demonstrando que a classificação normativa também pode produzir invisibilidades. A análise evidencia que a interpretação da lei deve permanecer conectada à realidade social e às formas concretas de discriminação.

Nessa perspectiva, a sensibilidade não deve ser aferida apenas pela etiqueta atribuída ao dado, mas pelo contexto, pela capacidade inferencial e pelo risco decorrente do tratamento. A proteção constitucional da pessoa exige indagar o que determinada operação permite descobrir, quais decisões podem ser tomadas a partir desse

conhecimento e quais grupos podem suportar de maneira desproporcional os seus efeitos.

3.1. O Regime Jurídico Reforçado e os Limites do Consentimento

O art. 11 da LGPD estabelece hipóteses específicas para o tratamento de dados pessoais sensíveis. Quando fundado no consentimento, este deve ser fornecido de forma específica e destacada, para finalidades específicas (Brasil, 2018). A exigência reforçada revela que uma autorização genérica não é suficiente para legitimar operações potencialmente invasivas.

O consentimento, contudo, não pode ser transformado em mecanismo de transferência integral da responsabilidade ao titular. Em ambientes digitais marcados por assimetria técnica e informacional, a pessoa frequentemente não dispõe de condições reais para compreender todas as etapas de processamento, correlação e reutilização de seus dados. A ANPD ressalta que consentimento pressupõe manifestação livre, informada e inequívoca, com efetiva possibilidade de escolha e revogação (ANPD, 2023).

A licitude do tratamento depende de requisitos que subsistem independentemente do consentimento. Finalidade, adequação e necessidade impedem a coleta indiscriminada e a reutilização incompatível; transparência permite conhecer aspectos relevantes da operação; segurança e prevenção impõem atuação anterior ao dano; não discriminação veda finalidades ilícitas ou abusivas; e responsabilização exige demonstração da eficácia das medidas adotadas.

Essa arquitetura normativa afasta uma compreensão meramente contratual da proteção de dados. A dignidade da pessoa humana impede que uma manifestação formal de vontade seja utilizada para neutralizar deveres objetivos do controlador. Em matéria de dados sensíveis, consentir não significa renunciar aos direitos fundamentais que estruturam o próprio sistema de proteção.

4. PERFILAMENTO, DECISÕES AUTOMATIZADAS E DISCRIMINAÇÃO ALGORÍTMICA

A inteligência artificial e o tratamento massivo de dados alteraram qualitativamente o problema jurídico. O dado deixou de ser relevante apenas pelo conteúdo que revela diretamente e passou a adquirir valor pelo conhecimento que sistemas computacionais conseguem produzir a partir de sua combinação. Perfilamento, pontuação, categorização e predição transformam informações dispersas em avaliações capazes de influenciar decisões sobre indivíduos.

Santos e Graminho (2024) demonstram que algoritmos já participam de decisões relevantes nas relações de trabalho, inclusive seleção, dispensa, monitoramento e avaliação. O problema, porém, ultrapassa esse setor: a mesma lógica pode alcançar crédito, seguros, saúde, publicidade, segurança e prestação de serviços. O elemento comum é a possibilidade de uma representação estatística do indivíduo passar a influenciar oportunidades concretas.

A promessa de neutralidade tecnológica deve ser recebida com cautela. Sistemas automatizados são desenvolvidos a partir de escolhas humanas, objetivos determinados e bases de dados

historicamente produzidas. Se os dados de treinamento refletem desigualdades anteriores, a automação pode reproduzi-las com aparência de objetividade matemática, vejamos:

> *Os algoritmos são treinados com dados históricos. Se esses dados forem tendenciosos contra certos indivíduos ou grupos, o algoritmo replicará o viés humano e aprenderá a discriminá-los (Moreira, 2022, p. 227 apud Santos; Graminho, 2024, p. 11).*

A passagem demonstra que o risco discriminatório não exige programação explicitamente preconceituosa. A desigualdade pode surgir da estrutura dos dados, da escolha das variáveis, dos critérios de otimização ou das correlações encontradas pelo modelo. Nesses casos, a aparência de neutralidade pode dificultar a identificação do tratamento desigual.

Santos e Graminho (2024) sistematizam formas de discriminação algorítmica que incluem erro estatístico, utilização de dados sensíveis, generalizações injustas e decisões limitadoras do exercício de direitos. Essa multiplicidade demonstra que retirar campos explicitamente sensíveis de uma base de dados não elimina, por si, o risco de discriminação.

A opacidade tecnológica amplia a dificuldade. Modelos complexos podem funcionar como caixas-pretas para o titular, que percebe a consequência da decisão sem conhecer adequadamente os critérios que conduziram a ela. Essa assimetria compromete a possibilidade de contestação e torna a transparência condição para o exercício de outros direitos.

A proteção jurídica deve alcançar tanto o dado de entrada quanto o resultado inferido e a decisão produzida. Se a dignidade impede a redução da pessoa a objeto informacional, também impede que classificações automatizadas juridicamente relevantes sejam aceitas como incontestáveis apenas porque derivam de sistemas tecnicamente sofisticados.

4.1. Não Discriminação, Transparência e Direito à Revisão

O princípio da não discriminação, previsto no art. 6º, IX, da LGPD, estabelece a impossibilidade de tratamento para fins discriminatórios ilícitos ou abusivos (Brasil, 2018). A norma deve ser interpretada em sentido material: não basta investigar a intenção do agente; é necessário avaliar os efeitos da operação e verificar se determinados grupos são submetidos a desvantagens injustificadas.

O art. 20 da LGPD assegura ao titular o direito de solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado que afetem seus interesses, inclusive decisões destinadas a definir perfil pessoal, profissional, de consumo e de crédito ou aspectos de sua personalidade (Brasil, 2018). Transparência e revisão funcionam, nesse contexto, como garantias instrumentais.

Santos e Graminho (2024) concluem que os princípios da não discriminação, transparência, responsabilização e prestação de contas, aliados à explicação e a sistemas de auditoria, oferecem instrumentos relevantes para reduzir riscos em decisões automatizadas. A explicabilidade, contudo, não se confunde com mera divulgação de código-fonte: a informação precisa permitir compreensão e contestação efetivas.

Essa compreensão aparece também na governança do Poder Judiciário. A Resolução CNJ nº 615/2025 estabeleceu diretrizes para desenvolvimento, monitoramento e uso responsável de inteligência artificial, com abordagem baseada em riscos, supervisão humana, auditabilidade e transparência. A experiência demonstra que eficiência tecnológica não afasta o controle jurídico; quanto maior o impacto do sistema, mais robustas devem ser as salvaguardas (CNJ, 2025).

5. EFETIVIDADE DA PROTEÇÃO: PREVENÇÃO, SEGURANÇA, GOVERNANÇA E RESPONSABILIZAÇÃO

O reconhecimento constitucional do direito à proteção de dados e a existência de regras específicas para informações sensíveis constituem avanços normativos relevantes, mas não garantem, isoladamente, proteção efetiva. Entre a norma e a realidade existe um espaço ocupado por escolhas organizacionais, arquitetura tecnológica, controles de acesso, políticas de retenção, treinamento, auditoria e resposta a incidentes.

A LGPD adota lógica preventiva. O art. 46 determina que agentes de tratamento adotem medidas técnicas e administrativas aptas a proteger dados contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou tratamento inadequado. O § 2º determina que essas medidas sejam observadas desde a fase de concepção do produto ou serviço (Brasil, 2018).

A proteção desde a concepção modifica a posição temporal do Direito. Em vez de atuar apenas depois do vazamento ou da discriminação, exige-se que riscos sejam considerados antes da

implementação do sistema. Essa prevenção é especialmente importante em relação a dados sensíveis porque determinados danos podem ser de difícil reversão.

A ANPD mantém instrumentos orientativos sobre segurança, agentes de tratamento, tratamento pelo Poder Público e proteção dos titulares. Esses documentos evidenciam que conformidade não se resume à existência de política de privacidade, mas exige medidas compatíveis com o risco das operações, definição de responsabilidades e mecanismos efetivos de atendimento aos direitos dos titulares (ANPD, 2024).

É necessário distinguir conformidade documental de conformidade substancial. Uma organização pode possuir termos e políticas formalmente elaborados e, ainda assim, coletar informações em excesso, conservar dados indefinidamente ou permitir acessos incompatíveis com as funções desempenhadas. A efetividade depende da correspondência entre o que é declarado e o que ocorre durante todo o ciclo de vida do dado.

5.1. Responsabilidade e Prestação de Contas Como Dever de Demonstração

O princípio da responsabilização e prestação de contas, previsto no art. 6º, X, exige demonstração da adoção de medidas eficazes capazes de comprovar a observância das normas de proteção de dados. A lógica desloca o agente da posição de simples destinatário de proibições para a condição de responsável por demonstrar a governança de suas operações.

Os arts. 42 e 44 da LGPD complementam essa estrutura ao disciplinar reparação de danos e irregularidade do tratamento que

descumpre a legislação ou não oferece a segurança legitimamente esperada pelo titular (Brasil, 2018). Segurança, portanto, não é mera recomendação técnica; integra o padrão jurídico de regularidade do tratamento.

Em sistemas de alto impacto, a prestação de contas deve envolver documentação das finalidades, bases legais, categorias de dados, critérios de acesso, medidas de segurança, testes, auditorias e procedimentos de revisão. Quando houver perfilamento ou inteligência artificial, a governança precisa abranger qualidade e representatividade dos dados, monitoramento de resultados e investigação de efeitos discriminatórios.

O CNJ oferece exemplo institucional dessa passagem da conformidade abstrata para a governança verificável. Sua política de inteligência artificial enfatiza monitoramento, supervisão humana e auditabilidade, reconhecendo que sistemas utilizados em contextos decisórios não podem operar sem mecanismos que permitam examinar seus resultados e atribuir responsabilidades (CNJ, 2025).

5.2. A Dignidade Humana Como Limite Material Ao Poder Informacional

De acordo com Sarlet, Mendes e Doneda (2022) a análise permite identificar duas funções complementares da dignidade da pessoa humana na proteção de dados pessoais. A primeira possui natureza interpretativa, uma vez que, diante de conceitos jurídicos indeterminados, lacunas normativas ou tecnologias não previstas expressamente pelo legislador, a dignidade constitui parâmetro para a interpretação das normas de modo a preservar a autonomia individual, a igualdade e o livre desenvolvimento da personalidade.

A segunda apresenta caráter limitador, pois estabelece que nem toda operação tecnologicamente possível pode ser considerada juridicamente admissível.

Nesse sentido, Sarlet (2015) compreende a dignidade humana como fundamento de proteção da pessoa contra práticas que comprometam sua autonomia e sua condição de sujeito de direitos. No campo informacional, essa compreensão exige que o tratamento de dados pessoais respeite os direitos fundamentais dos titulares, impedindo que o desenvolvimento tecnológico seja utilizado para justificar intervenções desproporcionais na esfera individual.

A capacidade técnica de inferir condições de saúde, prever comportamentos, estimar posicionamentos políticos ou classificar indivíduos segundo probabilidades estatísticas não constitui, por si só, autorização jurídica para a realização dessas operações. A legitimidade do tratamento depende da existência de fundamento jurídico adequado e da observância dos princípios da finalidade, adequação, necessidade, transparência e não discriminação, previstos no art. 6º da Lei nº 13.709/2018.

Conforme Bioni (2019), a proteção de dados pessoais deve ser compreendida a partir das relações de poder estabelecidas entre os agentes responsáveis pelo tratamento e os titulares, especialmente diante da possibilidade de utilização das informações para influenciar comportamentos e restringir escolhas individuais.

O problema contemporâneo da privacidade deixa, portanto, de se limitar à identificação das informações que devem permanecer secretas. Torna-se necessário examinar em que medida terceiros podem transformar dados relativos às pessoas em instrumentos de

previsão, classificação e tomada de decisões. Essa transformação evidencia que a proteção de dados não se restringe ao controle da divulgação de informações, abrangendo também os efeitos produzidos por seu processamento.

Nessa perspectiva, Rodotà (2008) sustenta que a proteção de dados pessoais representa uma dimensão fundamental da liberdade na sociedade contemporânea, especialmente diante da ampliação das possibilidades de vigilância, controle e utilização econômica das informações individuais.

A pessoa humana não pode ser reduzida ao perfil construído por sistemas automatizados a partir de seus dados. Os perfis digitais constituem representações estatísticas e contextuais, incapazes de reproduzir integralmente a complexidade da identidade individual. Sua utilização como fundamento exclusivo de decisões relevantes pode produzir classificações discriminatórias e limitar oportunidades futuras com base em comportamentos anteriormente registrados.

Como observa Bioni (2019), o tratamento de dados pessoais possui repercussões que ultrapassam a esfera individual, alcançando questões relacionadas à igualdade e à autodeterminação informativa. Dessa forma, a dignidade humana exige a preservação de condições efetivas para o exercício da autonomia, a contestação de decisões e a possibilidade de transformação da própria trajetória pessoal, em consonância com a proteção constitucional dos dados pessoais estabelecida pela Emenda Constitucional nº 115/2022.

6. CONSIDERAÇÕES FINAIS

A pesquisa buscou responder de que forma o princípio da dignidade da pessoa humana fundamenta a proteção dos dados pessoais

sensíveis no ambiente digital e quais mecanismos jurídicos são capazes de assegurar essa tutela de maneira efetiva. O percurso demonstrou que a resposta não pode ser construída apenas a partir do sigilo ou da ideia tradicional de privacidade.

Na sociedade informacional, dados pessoais integram a representação digital do indivíduo e podem interferir na maneira como ele é reconhecido, classificado e submetido a decisões. A proteção dos dados sensíveis corresponde, por isso, à proteção de dimensões da própria personalidade e possui estreita relação com igualdade, autonomia e não discriminação.

Verificou-se que o regime especial previsto pela LGPD encontra fundamento no potencial agravado de determinadas informações produzirem exposição, estigmatização e exclusão. Entretanto, a evolução tecnológica desafia uma leitura estritamente formal do rol legal, pois inferências produzidas a partir de dados aparentemente neutros podem revelar características sensíveis e gerar consequências equivalentes às decorrentes do tratamento direto dessas informações.

O consentimento mostrou-se importante, mas insuficiente como eixo exclusivo de legitimação. A assimetria informacional existente nas relações digitais exige deveres objetivos de finalidade, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização.

A análise das decisões automatizadas demonstrou que a discriminação pode decorrer da estrutura dos dados e dos modelos, mesmo sem intenção explícita de excluir. Por essa razão, transparência, revisão, explicabilidade, auditoria e supervisão

humana devem ser compreendidas como instrumentos de efetivação da igualdade.

Conclui-se que a dignidade da pessoa humana desempenha função dupla: fundamenta a proteção informacional e estabelece limite material ao poder de coletar, correlacionar, inferir e decidir a partir de dados. A tecnologia pode ampliar eficiência e inovação, mas não autoriza a conversão do indivíduo em objeto passivo de classificação.

A resposta ao problema de pesquisa é, portanto, afirmativa no sentido de que o ordenamento brasileiro dispõe de mecanismos jurídicos relevantes para a tutela dos dados sensíveis, especialmente a constitucionalização da proteção de dados, o regime diferenciado da LGPD, os princípios do art. 6º, a revisão de decisões automatizadas, os deveres de segurança, a responsabilização e os instrumentos de governança. Sua efetividade, contudo, depende de interpretação material e aplicação preventiva, capazes de acompanhar novas formas de inferência e discriminação.

Em síntese, quanto maior a capacidade tecnológica de conhecer, prever e classificar pessoas, maior deve ser a capacidade jurídica de assegurar que esse conhecimento permaneça subordinado à autonomia, à igualdade e ao livre desenvolvimento da personalidade. É nesse ponto que a dignidade humana deixa de funcionar como referência abstrata e passa a operar como critério concreto de legitimidade do tratamento de dados.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Dhiego Melo Job de. O direito à privacidade e à proteção de dados pessoais: repercussões da superação do sigilo como único instrumento de tutela da dignidade humana nas exceções do art. 4º

da LGPD. **Revista de Estudos Jurídicos UNESP,** Franca, v. 26, n. 44, 2023. DOI: 10.22171/rej.v26i44.3563.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia orientativo: tratamento de dados pessoais pelo Poder Público.** Brasília, DF: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_orientativo_tratamento_de_dados_pessoais_pelo_poder_publico. Acesso em: 6 out. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Materiais educativos e publicações.** Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes. Acesso em: 6 out. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Perguntas frequentes.** Brasília, DF: ANPD, 2026. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes. Acesso em: 6 out. 2026.

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

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 jun. 2026.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022.** Brasília, DF: Presidência da República, 2022. Disponível em:

https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 26 jun. 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet.** Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 8 jul. 2026.

BRASIL**. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 jul. 2026.

CARMO, Jocimauro Bento do. **Autodeterminação informativa como um instrumento de aplicação da função social do direito e sua relação com a dignidade da pessoa humana.** Contribuciones a las Ciencias Sociales, v. 17, n. 7, 2024. DOI: 10.55905/revconv.17n.7-408. Disponível em: https://ojs.revistacontribuciones.com/ojs/index.php/clcs/article/view/8842. Acesso em: 03 de out. 2026.

CEZARINO, Maraisa Rosa. **A institucionalização da invisibilidade da identidade de gênero: análise das audiências públicas do processo legislativo da LGPD.** 2024. Dissertação (Mestrado em Direito) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2024. DOI: 10.11606/D.2.2024.tde-29052024-144806. Disponível em: https://teses.usp.br/teses/disponiveis/2/2139/tde-29052024-144806/pt-br.html. Acesso em: 6 out. 2026.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Resolução nº 615, de 11 de março de 2025.** Brasília, DF: CNJ, 2025. Disponível em:

https://atos.cnj.jus.br/atos/detalhar/6001. Acesso em: 6 out. 2026.

COSTA, Ramon Silva. A proteção dos dados pessoais sensíveis sobre vida sexual a partir do Direito Antidiscriminatório. 2024. Tese (Doutorado em Direito) - Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2024. Disponível em: https://pos.jur.puc-rio.br/br/documentos/19/teses. Acesso em: 6 out. 2026.

GIMENEZ, Carina Magda de Souza. **Dados pessoais sensíveis: rol exemplificativo ou taxativo? Uma análise da categoria especial à luz da LGPD.** 2025. 85 f. Dissertação (Mestrado Profissional em Direito) - Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, São Paulo, 2025. Disponível em: https://repositorio.idp.edu.br/handle/123456789/5422. Acesso em: 6 out. 2026.

MELO, Renan; ALVIM, Marcia Cristina de Souza. Caminhos para a proteção da dignidade da pessoa humana na sociedade de dados. **Revista Internacional CONSINTER de Direito,** n. 17, 2023. DOI: 10.19135/revista.consinter.00017.02. Disponível em: https://revistaconsinter.com/index.php/ojs/1702. Acesso em: 05 out. 2026.

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

SANTOS, Rodrigo Coimbra; GRAMINHO, Vivian Maria Caxambu. Discriminação algorítmica nas relações de trabalho e princípios da Lei Geral de Proteção de Dados. Sequência**: Estudos Jurídicos e Políticos,** Florianópolis, v. 45, n. 96, p. 1-31, 2024. DOI: 10.5007/2177-

7055.2024.e96294. Disponível em: https://www.scielo.br/j/seq/a/9FGhvr75HYSdGMRfKnJ9FZd/?lang=pthttps://periodicos.ufsc.br/index.php/sequencia/article/view/96294. Acesso em: 6 out. 2026.

SARLET, Ingo Wolfgang; MENDES, Laura Schertel; DONEDA, Danilo. Estudos sobre proteção de dados pessoais. São Paulo: Saraiva Educação, 2022. E-book. Disponível em: https://books.google.com/books?id=iiZmEAAAQBAJ. Acesso em: 9 out. 2026.

SARLET, Ingo Wolfgang**. Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988.** 10. ed. rev., atual. e ampl. Porto Alegre: Livraria do Advogado, 2015.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, série L, n. 119, p. 1–88, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=pt. Acesso em: 21 out. 2026.

YAEGASHI, João Gabriel; OTERO, Cleber Sanfelici; MAIA, Robson Borges. A influência da Volkszählungsurteil no ordenamento jurídico brasileiro: um norte para a construção do direito à proteção de dados pessoais para a tutela da personalidade. **Opinión Jurídica,** v. 23, n. 49, 2024. DOI: 10.22395/ojum.v23n49a32. Disponível em: https://revistas.udem.edu.co/index.php/opinion/pt_BR/article/view/4172/3687. Acesso em: 03 set. 2026.

ZANINI, Leonardo Estevam de Assis; QUEIROZ, Odete Novais Carneiro. O princípio fundamental da dignidade da pessoa humana e a sua atuação como cláusula geral de tutela da personalidade. **Revista do Tribunal Regional Federal da 3ª Região,** São Paulo, v. 34, n. 158, p. 211-234, 2023. DOI: 10.65674/rev-trf3.v34i158.110. Disponível em: https://revista.trf3.jus.br/index.php/rtrf3/pt_BR/article/view/110. Acesso em: 04 out. 2026.

---

[1] Acadêmico de Direito. E-mail: Artigo apresentado ao Centro Universitário Unisapiens como requisito para obtenção do título de Bacharel em Direito. Porto Velho/RO, 2026. E-mail: acesse o artigo original para visualizar o e-mail

[2] Professor Orientador. Doutorando em Direito pela Pontifícia Universidade Católica do Paraná (PUCPR), em convênio com a Faculdade Católica de Rondônia (FCR). Mestre em Administração pela Universidade Federal de Rondônia (UNIR). Auditor Fiscal da SEFIN/RO, com experiência em gestão pública e controle interno. Professor do curso de Direito do Centro Universitário Unisapiens e orientador do presente artigo. E-mail: acesse o artigo original para visualizar o e-mail.