aurum
Revista Multidisciplinar

ISSN: 3085-7783

GOVERNANÇA ÉTICA DE DADOS NA ERA DIGITAL: PRIVACIDADE, DIGNIDADE HUMANA E LIMITES DA MEDIAÇÃO ALGORÍTMICA

ETHICAL DATA GOVERNANCE IN THE DIGITAL AGE: PRIVACY, HUMAN DIGNITY AND THE LIMITS OF ALGORITHMIC MEDIATION

https://doi.org/10.63330/armv2n3-018

Submetido em: 08/04/2026 e Publicado em: 14/04/2026

Jean Carlos Viana Barreto da Cunha
Pós-graduando (Especialização em Ciência de Dados e Inteligência Artificial) – Pós-graduado em Gestão de Pessoas pela Faculdade Única de Ipatinga. Instituição acadêmica: Faculdade Iguaçu
E-mail: vianajeanjean@gmail.com
Lattes: https://lattes.cnpq.br/4083668268812578
ORCID: https://orcid.org/0009-0003-9520-4718

RESUMO

Este artigo analisa os desafios éticos da governança de dados na era digital, com ênfase na privacidade, na proteção de dados pessoais e na dignidade humana, diante da ampliação da coleta massiva de informações, da circulação intensiva de dados e da mediação algorítmica das relações sociais. O objetivo consiste em examinar de que modo a expansão das tecnologias digitais compromete a proteção desses valores e quais parâmetros éticos e normativos podem contribuir para sua preservação. Metodologicamente, trata-se de pesquisa qualitativa, de natureza bibliográfica e documental, desenvolvida a partir da análise de obras teóricas, artigos científicos e marcos normativos nacionais e internacionais diretamente relacionados ao tema. A análise indica que a expansão do uso de serviços digitais não assegura, por si só, governança adequada da informação, pois persistem assimetrias informacionais, baixa transparência nos tratamentos automatizados e limitações no controle exercido pelos usuários sobre seus dados. Conclui-se que a governança ética de dados depende da articulação entre transparência, accountability, gestão de riscos informacionais e mecanismos concretos de proteção capazes de qualificar o uso de dados e reduzir efeitos adversos da mediação algorítmica.

Palavras-chave: Ética digital; Governança de dados; Privacidade; Proteção de dados; Mediação algorítmica.

ABSTRACT

This article analyzes the ethical challenges of data governance in the digital age, with emphasis on privacy, personal data protection, and human dignity in the context of large-scale information collection, intensive data circulation, and algorithmic mediation of social relations. Its objective is to examine how the expansion

of digital technologies compromises the protection of these values and which ethical and normative parameters may contribute to their preservation. Methodologically, the study adopts a qualitative bibliographic and documentary approach based on the analysis of theoretical works, scientific articles, and national and international normative references directly related to the topic. The analysis indicates that the expansion of digital services does not, by itself, ensure adequate information governance, since informational asymmetries, limited transparency in automated processing, and restrictions on users' control over their own data remain significant. It is concluded that ethical data governance depends on the articulation of transparency, accountability, informational risk management, and concrete protection mechanisms capable of improving data use practices and reducing adverse effects associated with algorithmic mediation.

Keywords: Data governance; Data protection; Digital ethics; Privacy; Algorithmic mediation.

1 INTRODUÇÃO

A era digital consolidou um ambiente social marcado pela circulação intensiva de dados, pela mediação algorítmica das interações humanas e pela crescente dependência de plataformas tecnológicas para o exercício de atividades ordinárias, como comunicação, trabalho, consumo, educação e participação pública. Nesse cenário, a discussão ética já não pode ser tratada em termos abstratos ou meramente declaratórios, pois as escolhas técnicas incorporadas aos sistemas digitais passaram a afetar diretamente práticas de gestão da informação, padrões de transparência, formas de controle e relações de poder no ambiente digital. A governança ética de dados, portanto, deixa de ser apenas diretriz abstrata e passa a constituir exigência prática para ambientes digitais baseados em coleta, tratamento, cruzamento e exploração de dados.

Entre os diversos problemas que emergem nesse contexto, destacam-se aqueles relacionados à privacidade, à proteção de dados pessoais e à dignidade humana. A privacidade, antes frequentemente compreendida sob a ótica restrita do segredo ou do resguardo da vida íntima, passou a ser pressionada por mecanismos permanentes de vigilância, perfilamento e previsão comportamental que alcançam não apenas o espaço individual, mas também as condições de autonomia e liberdade dos sujeitos. Doneda (2021) demonstra que a proteção de dados não se limita à exigência formal de conformidade, mas integra práticas de governança voltadas ao controle informacional, à redução de assimetrias e à qualificação do uso de dados em sistemas digitais.

A centralidade dos dados pessoais na economia digital agravou esse problema. Modelos de negócio baseados na extração massiva de informações, na opacidade dos tratamentos automatizados e na indução de comportamentos revelam que a inovação tecnológica não é eticamente neutra. Ao contrário, a

infraestrutura digital contemporânea tende a converter experiências humanas em insumos econômicos, reforçando práticas de vigilância e aprofundando desequilíbrios entre aqueles que produzem dados e aqueles que os capturam, organizam e monetizam. Por isso, discutir governança ética de dados na era digital exige examinar criticamente como a racionalidade técnica e econômica das plataformas pode colidir com valores fundamentais, sobretudo quando a eficiência, a personalização e a previsibilidade passam a se sobrepor à autonomia, à transparência e ao controle informacional dos titulares dos dados (Mendes; Fonseca, 2020).

No contexto brasileiro, a governança de dados passou a contar com referências institucionais e regulatórias mais definidas nos últimos anos. O Marco Civil da Internet estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil; a Lei Geral de Proteção de Dados Pessoais (LGPD) disciplinou o tratamento de dados pessoais, inclusive em meios digitais; e a Emenda Constitucional nº 115 inseriu a proteção de dados pessoais, inclusive nos meios digitais, no rol dos direitos e garantias fundamentais. Esse conjunto normativo demonstra que a discussão sobre privacidade e proteção de dados já não pode ser reduzida à questão periférica do direito digital, mas deve ser compreendida como dimensão estruturante da tutela da pessoa humana em uma sociedade orientada por fluxos informacionais e decisões automatizadas (Brasil, 2014; Brasil, 2018; Brasil, 2022).

Além da dimensão nacional, o debate internacional também aponta para a necessidade de subordinar o desenvolvimento tecnológico a parâmetros éticos explícitos. A Recomendação da UNESCO sobre a Ética da Inteligência Artificial, adotada em 2021, reafirma a centralidade da dignidade humana, dos direitos humanos, da transparência, da responsabilização e da supervisão humana como fundamentos indispensáveis para o uso legítimo e socialmente aceitável de sistemas inteligentes. Tal orientação reforça a compreensão de que, em ambientes digitais altamente automatizados, a ética não pode ser concebida como adorno discursivo da inovação, mas como critério material de limitação do poder tecnológico e de preservação das condições mínimas de justiça e humanidade nas relações mediadas por dados e algoritmos (UNESCO, 2021).

É nesse quadro que se insere o presente artigo, cujo problema de pesquisa pode ser formulado nos seguintes termos: em que medida a intensificação da coleta de dados pessoais e da mediação algorítmica compromete a governança ética de dados na era digital, especialmente no que se refere à privacidade, à proteção de dados e à dignidade humana?

O objetivo geral do estudo consiste em analisar como a privacidade, a proteção de dados pessoais e a dignidade humana se afirmam como eixos centrais da governança ética de dados na era digital. De modo específico, busca-se discutir os fundamentos teóricos da ética digital, examinar os principais riscos éticos decorrentes da coleta massiva de dados e da mediação algorítmica, bem como identificar o papel de referências regulatórias e diretrizes internacionais na contenção desses riscos. A justificativa da pesquisa

reside na relevância social, jurídica e acadêmica do tema, sobretudo em um contexto no qual a transformação digital avança com rapidez superior à capacidade de compreensão crítica e de resposta institucional, produzindo zonas de vulnerabilidade que afetam diretamente os direitos fundamentais.

Quanto ao percurso metodológico, trata-se de pesquisa qualitativa, de natureza bibliográfica e documental, desenvolvida a partir da revisão e análise interpretativa de obras teóricas, artigos científicos e marcos normativos relacionados à ética digital, à privacidade, à proteção de dados e à dignidade humana.

A análise desenvolvida no artigo parte da compreensão de que a ética digital não se limita a formulações abstratas sobre conduta, mas se projeta sobre estruturas concretas de governança, tratamento de dados e responsabilização institucional. Com base nessa premissa, o texto articula fundamentos teóricos, marcos normativos e evidências documentais para examinar como privacidade, proteção de dados e dignidade humana permanecem no centro dos desafios éticos da era digital. Ao final, retoma-se o problema da pesquisa para sustentar que a fidelidade aos princípios éticos na era digital depende da conversão desses princípios em limites materiais efetivos ao exercício do poder tecnológico.

2 REFERENCIAL TEÓRICO

A discussão sobre governança ética de dados na era digital exige superar a compreensão restrita de privacidade como simples resguardo da intimidade. Na sociedade digital, a questão central já não se limita à proteção contra exposições indevidas, mas envolve o controle sobre a coleta, o tratamento, o compartilhamento e a reutilização de informações pessoais em larga escala. Nesse cenário, a privacidade deixa de ser apenas uma barreira defensiva e passa a ser compreendida como condição de autonomia, liberdade e autodeterminação informativa. Em outras palavras, a transformação tecnológica deslocou a discussão do campo do segredo para o campo do poder informacional (Floridi, 2013).

Capurro (2004) contribui para essa mudança ao sustentar que a ética da informação abrange os problemas éticos relacionados às tecnologias digitais e à reconfiguração das relações humanas por meio delas. Floridi (2013), por sua vez, amplia esse horizonte ao defender que a vida contemporânea ocorre em uma “infosfera”, na qual a pessoa também se constitui informacionalmente. Essa formulação é decisiva porque permite compreender que a violação da privacidade não se resume à divulgação de conteúdos íntimos, mas inclui intervenções sobre a identidade informacional do sujeito. Assim, o problema ético não está apenas no acesso indevido à informação, mas na própria reorganização do ambiente social em torno da captura e circulação contínua de dados.

No debate brasileiro sobre proteção de dados, Doneda (2021) demonstra que o tratamento automatizado de dados cria riscos específicos porque viabiliza coleta, classificação, cruzamento e uso de informações em múltiplos contextos, muitas vezes sem conhecimento efetivo do titular. Nessa perspectiva, a proteção de dados não se reduz a requisito formal, mas passa a integrar mecanismos de controle

informacional e limitação de usos excessivos ou opacos. A relevância ética dessa leitura é direta: quando o indivíduo é transformado em conjunto de dados permanentemente observável, a questão que se impõe já não é apenas a da intimidade, mas a da preservação de sua condição de sujeito.

Nessa perspectiva, a LGPD consolidou princípios como finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização, oferecendo parâmetros relevantes para qualificar práticas de tratamento de dados em ambientes digitais (Brasil, 2018).

O peso desse dispositivo está em mostrar que a proteção de dados não se esgota na autorização formal do titular. A própria lei reconhece que o tratamento deve obedecer a limites materiais, o que revela uma aproximação entre o campo jurídico e a exigência ética de contenção do poder informacional. Por isso, fidelidade aos princípios éticos, no ambiente digital, não pode significar apenas respeito abstrato à pessoa, mas proteção concreta contra tratamentos excessivos, opacos e potencialmente discriminatórios (Doneda, 2021).

Quadro 1: Relação entre privacidade, proteção de dados e dignidade humana

Categoria	**Conteúdo central**	**Risco ético principal**
Privacidade	Resguardo da esfera pessoal e da autonomia do sujeito	Vigilância contínua e perda de controle informacional
Proteção de dados	Limitação e controle sobre coleta, uso e circulação de informações pessoais	Tratamento opaco, excessivo ou indevido
Dignidade humana	Reconhecimento da pessoa como fim em si mesma	Redução do sujeito a objeto de monitoramento e inferência

Fonte: Adaptado de Doneda (2021)

2.1 CONSENTIMENTO, ASSIMETRIA E TUTELA DA DIGNIDADE HUMANA

A proteção ética da pessoa na era digital exige enfrentar um ponto central: a profunda assimetria informacional existente entre titulares de dados e agentes que os coletam e tratam. A economia digital é estruturada por plataformas e sistemas que extraem valor da observação contínua de comportamentos, preferências, deslocamentos e interações. Nesse contexto, o dado pessoal deixa de ser simples registro e passa a funcionar como matéria-prima para segmentação, predição e modulação de condutas. A dignidade humana é diretamente problematizada quando o sujeito perde inteligibilidade sobre o que é coletado a seu respeito, para quais finalidades essas informações são usadas e com que efeitos elas retornam sobre sua vida social (Zuboff, 2019).

Zuboff (2019) é decisiva ao demonstrar que a lógica contemporânea de exploração de dados não constitui prática periférica, mas elemento central de um modelo econômico assentado na captura da

experiência humana. Seu argumento mostra que o problema ético não está apenas no excesso de tecnologia, mas na conversão sistemática da vida cotidiana em fonte de extração informacional. Isso tem implicações profundas para a dignidade humana, porque desloca o indivíduo da condição de sujeito de direitos para a condição de objeto de observação, cálculo e previsão.

No debate jurídico, Mendes e Fonseca (2020) aprofundam essa crítica ao problematizar a centralidade do consentimento na proteção de dados pessoais. Os autores demonstram que, em ambientes informacionais estruturalmente assimétricos, consentir não equivale necessariamente a controlar. O titular, em regra, não decide em condições plenamente livres e informadas, seja pela opacidade das políticas de tratamento, seja pela dependência concreta dos serviços digitais, seja pela complexidade técnica dos processos de análise de dados. A autonomia formal, nesse cenário, não basta para assegurar proteção material.

Essa crítica é relevante porque desmonta uma justificativa recorrente no discurso tecnológico: a de que a aceitação dos termos de uso legitimaria, por si só, qualquer tratamento posterior. Não legitimaria. Em termos éticos, a mera anuência formal não neutraliza a desigualdade estrutural entre usuário e plataforma. Por isso, a governança ética de dados exige mais do que consentimento; exige transparência, limitação de finalidade, proporcionalidade, segurança e responsabilização. A dignidade humana, nesse ponto, funciona como categoria de contenção, impedindo que a pessoa seja tratada como simples fornecedora passiva de dados (Doneda, 2021).

A própria crítica dos autores é clara ao mostrar que há “assimetria de poderes” entre o titular dos dados e os agentes de tratamento (Mendes; Fonseca, 2020, p. 516). Essa observação é central para o presente artigo, porque demonstra que a ética digital não pode permanecer presa a uma noção formalista de autonomia. Em ambientes digitais, a proteção da pessoa humana depende de salvaguardas institucionais e normativas que reduzam o desequilíbrio entre quem entrega os dados e quem detém os meios técnicos e econômicos de processá-los.

2.2 MEDIAÇÃO ALGORÍTMICA, TRANSPARÊNCIA E RESPONSABILIDADE INSTITUCIONAL

A discussão torna-se ainda mais complexa quando os dados coletados passam a alimentar sistemas algorítmicos que classificam, recomendam, hierarquizam e influenciam decisões. Nesse nível, o sujeito não é afetado apenas pela coleta de informações, mas também por inferências e correlações produzidas a partir dessas informações. A mediação algorítmica altera a dinâmica do problema ético porque introduz um grau elevado de opacidade: muitas vezes, o indivíduo não sabe quais critérios foram utilizados, quais dados foram correlacionados e quais impactos concretos decorrem desse processamento. Isso compromete não apenas a transparência, mas também a possibilidade de contestação e responsabilização (Rossetti; Angeluci, 2021).

Rossetti e Angeluci (2021) mostram que a ética algorítmica se estrutura em torno de problemas como opacidade, falibilidade, viés, discriminação, privacidade, autonomia e responsabilidade. O ponto forte dessa abordagem está em afastar a ficção da neutralidade técnica. Algoritmos não são instrumentos neutros que apenas executam comandos; eles operam sobre bases de dados situadas historicamente e produzem efeitos reais sobre pessoas concretas. Quando usados em processos de recomendação, ranqueamento, filtragem ou decisão, podem reforçar desigualdades, cristalizar vieses e dificultar a compreensão dos critérios que produzem determinados resultados.

Nesse cenário, transparência e responsabilidade deixam de ser atributos acessórios e passam a constituir exigências éticas centrais. A Recomendação da UNESCO sobre a Ética da Inteligência Artificial reforça essa direção ao associar proteção da dignidade humana, direitos humanos, privacidade, supervisão humana e responsabilização como fundamentos da governança ética dos sistemas de IA (UNESCO, 2021). Na mesma linha, os princípios da OCDE para inteligência artificial vinculam a legitimidade dos sistemas automatizados ao respeito a direitos fundamentais, transparência e accountability (OECD, 2024). O argumento convergente é inequívoco: eficiência técnica, sozinha, não legitima mediação algorítmica.

Por isso, a fidelidade aos princípios éticos na era digital exige que o sujeito permaneça no centro da proteção normativa. Isso implica reconhecer que privacidade, proteção de dados e dignidade humana não são temas paralelos, mas dimensões interdependentes de um mesmo problema. Quanto maior a capacidade de coletar, processar, prever e influenciar comportamentos, maior deve ser a exigência de limites materiais, supervisão humana, transparência proporcional e responsabilização institucional. Sem esses elementos, a ética digital se reduz a discurso e perde sua função crítica e normativa (UNESCO, 2021).

3 METODOLOGIA

O presente estudo caracteriza-se como pesquisa qualitativa, de natureza básica, com finalidade exploratória e analítico-interpretativa, desenvolvida por meio de pesquisa bibliográfica e documental. Esse delineamento mostra-se adequado ao objetivo do artigo, que consiste em analisar, sob perspectiva crítica, a governança ética de dados na era digital, com ênfase na privacidade, na proteção de dados e na dignidade humana. Em razão da natureza do problema investigado, não se buscou mensuração estatística nem levantamento de campo, mas interpretação fundamentada de referenciais teóricos e normativos pertinentes ao tema. A pesquisa qualitativa, nesse contexto, permite compreender significados, valores, estruturas argumentativas e implicações éticas presentes nos textos analisados (Minayo, 2014).

Por se tratar de pesquisa bibliográfica e documental, o estudo não opera com população e amostra em sentido estatístico. O corpus analítico foi constituído de forma intencional, com base em critérios de pertinência temática, relevância acadêmica e centralidade normativa, reunindo obras teóricas, artigos científicos e documentos jurídicos diretamente relacionados à ética digital, à proteção de dados, à

privacidade e à mediação algorítmica. No plano documental, foram selecionados textos normativos e institucionais centrais para a discussão do tema, como a Constituição Federal, o Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais e documentos internacionais voltados à ética digital e à inteligência artificial. Assim, a composição do corpus não obedeceu a critério numérico, mas à capacidade dos materiais escolhidos de sustentar, com densidade teórica e jurídica, o problema formulado no artigo (Severino, 2017).

A coleta de dados foi realizada por meio de levantamento bibliográfico e documental, seguido de leitura seletiva, leitura analítica e fichamento dos materiais escolhidos. Inicialmente, procedeu-se à identificação das obras e documentos mais diretamente vinculados ao tema do estudo. Em seguida, os textos foram selecionados conforme sua aderência aos eixos centrais da pesquisa: privacidade, proteção de dados e dignidade humana na era digital. Na etapa de fichamento, foram extraídos conceitos, argumentos, categorias analíticas e dispositivos normativos relevantes para a construção do referencial teórico e para a discussão do problema de pesquisa. Esse procedimento permitiu organizar o material de forma sistemática, evitando dispersão temática e garantindo unidade argumentativa ao artigo (GIL, 2019).

A forma de análise dos dados baseou-se em análise qualitativa de conteúdo, em perspectiva temática, articulada à interpretação bibliográfica e documental. Nesse processo, os materiais selecionados foram examinados com o objetivo de identificar convergências, divergências e complementaridades entre os autores e os documentos normativos analisados.

Desse modo, a metodologia adotada assegura coerência entre o objeto investigado, os materiais selecionados e a forma de análise empregada. Ao optar por uma abordagem qualitativa, bibliográfica e documental, o estudo buscou examinar o tema com rigor conceitual e normativo, sem extrapolar os limites de um artigo científico de caráter teórico-analítico.

4 ANÁLISE E DISCUSSÃO

A análise desenvolvida ao longo deste artigo permite afirmar que a governança ética de dados na era digital não pode ser compreendida apenas como adesão abstrata a valores como privacidade, liberdade e dignidade humana. Esta análise indica que, no ambiente digital contemporâneo, a efetividade desses princípios depende da existência de mecanismos concretos de proteção, controle e responsabilização capazes de limitar o poder informacional exercido por plataformas, sistemas algorítmicos e estruturas de tratamento de dados. Em outros termos, o avanço da digitalização amplia direitos e oportunidades, mas também intensifica riscos éticos relacionados à vigilância, à opacidade, à assimetria informacional e à objetificação da pessoa. Essa leitura é compatível com a crítica formulada por Doneda (2021), para quem o tratamento de dados pessoais não deve ser tratado como operação neutra, mas como atividade potencialmente lesiva à personalidade, e com a análise de Mendes e Fonseca (2020), que demonstram a

insuficiência do consentimento como fundamento isolado de legitimidade em ambientes estruturalmente assimétricos.

Os dados oficiais reforçam esse diagnóstico. A Pesquisa TIC Domicílios 2024 mostra que o uso da Internet já alcança parcela amplíssima da população, mas isso não significa, automaticamente, apropriação crítica nem proteção efetiva dos dados pessoais. A Tabela 1 sintetiza indicadores centrais desse cenário.

Tabela 1: Indicadores selecionados sobre acesso, proteção e uso digital no Brasil (2024)

Indicador	**Base de referência**	**Valor**
Usuários de Internet	População total	84%
Usuários de Internet	Total estimado de pessoas	159 milhões
Não usuários de Internet	Total estimado de pessoas	29 milhões
Usuários que adotaram medidas de segurança para proteger dispositivos e contas	Usuários de Internet	48%
Usuários que mudaram configurações de privacidade para limitar o compartilhamento de dados	Usuários de Internet	38%
Usuários que utilizaram governo eletrônico	Usuários de Internet com 16 anos ou mais	61%

Fonte: CGI.br, 2024.

A tabela torna visível um ponto central da discussão: a universalização progressiva do acesso não elimina desigualdades qualitativas no modo como a população se insere no ambiente digital.

Nesse sentido, os resultados do estudo confirmam a hipótese de que a governança ética de dados depende menos da expansão quantitativa da conectividade e mais da criação de condições normativas e institucionais que garantam controle informacional, transparência e responsabilização. A diferença entre os 84% de usuários da Internet e os 38% que alteram configurações de privacidade é particularmente eloquente, pois sugere que o uso da rede se expandiu de forma muito mais rápida do que a internalização de práticas mínimas de autoproteção informacional. Essa conclusão, embora inferencial, encontra apoio direto nos dados oficiais analisados.

Outro aspecto relevante refere-se à dimensão desigual da digitalização. A própria TIC Domicílios 2024 mostra que o uso de governo eletrônico varia significativamente conforme escolaridade, faixa etária, classe e nível de conectividade. Entre usuários com Ensino Superior, 83% utilizaram serviços públicos

online, enquanto, entre os com Ensino Fundamental, esse percentual foi de 39%. Do mesmo modo, o uso foi menor entre pessoas das classes DE (43%) e entre indivíduos com 60 anos ou mais (38%). Esses dados mostram que a digitalização de serviços públicos, embora possa ampliar eficiência e alcance, também corre o risco de reproduzir ou aprofundar desigualdades preexistentes quando não acompanhada por políticas de inclusão, acessibilidade e simplificação. Em chave ética, isso significa que a proteção da dignidade humana não pode ser pensada apenas como limitação de abusos informacionais privados, mas também como garantia de acesso equitativo e não excludente às mediações digitais que atravessam a cidadania contemporânea.

A discussão teórica construída nas seções anteriores encontra, portanto, confirmação analítica nos materiais examinados. Doneda (2021) já advertia que o risco inerente ao tratamento automatizado de dados exige reconhecer a proteção de dados como instrumento essencial de tutela da pessoa humana. O trecho a seguir sintetiza, com precisão, essa perspectiva e serve como eixo interpretativo dos resultados obtidos:

> O tratamento de dados pessoais, em particular por processos automatizados, é, no entanto, uma atividade de risco. Risco que se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais, na eventualidade desses dados não serem corretos e representarem erroneamente seu titular, em sua utilização por terceiros sem o conhecimento deste, somente para citar algumas hipóteses reais. Daí resulta ser necessária a instituição de mecanismos que possibilitem à pessoa deter conhecimento e controle sobre seus próprios dados que, no fundo, são expressão direta de sua própria personalidade. Por este motivo, a proteção de dados pessoais é considerada em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e como um direito fundamental. (Doneda, 2021, p. 92).

Essa formulação é particularmente importante porque permite interpretar os dados apresentados não como estatísticas isoladas, mas como sinais concretos de um problema estrutural. Se a proteção de dados constitui instrumento de defesa da personalidade, então a baixa incidência de práticas de configuração de privacidade e a persistência de desigualdades no acesso qualificado aos serviços digitais não são questões meramente técnicas: elas afetam diretamente a possibilidade de exercício autônomo da liberdade e a preservação da dignidade humana. O mesmo vale para a mediação algorítmica. A UNESCO afirma que a privacidade deve ser protegida e promovida ao longo de todo o ciclo de vida da inteligência artificial, associando essa exigência à necessidade de estruturas adequadas de proteção de dados e responsabilização. Logo, as análises do presente estudo apontam que a governança ética de dados na era digital não se esgota na previsão legal desses direitos, mas depende de sua efetiva tradução em práticas, competências e mecanismos de governança.

Em síntese, os resultados e a discussão convergem para três constatações principais. A primeira é que a digitalização da vida social já é estrutural, o que torna insuficiente qualquer abordagem ética marginal ou secundária. A segunda é que privacidade, proteção de dados e dignidade humana são dimensões interdependentes: fragilizar uma delas compromete as demais. A terceira é que a simples expansão do

acesso digital não garante proteção ética, pois persistem déficits de segurança, de controle informacional e de inclusão qualificada. Disso decorre a principal conclusão desta seção: na era digital, a governança ética de dados somente se realiza quando o avanço tecnológico é acompanhado por proteção material da pessoa, transparência nos tratamentos de dados, redução das assimetrias informacionais e responsabilização institucional pelos impactos produzidos.

5 CONCLUSÃO

O artigo demonstrou que a governança ética de dados na era digital depende de práticas concretas de transparência, controle informacional, responsabilização e supervisão dos usos tecnológicos de dados. Verificou-se que o avanço das tecnologias digitais amplia oportunidades de conexão, automação e eficiência, mas também produz opacidade, assimetrias e riscos que não podem ser enfrentados apenas por adesão formal a políticas de uso ou por referências regulatórias abstratas.

Conclui-se que a qualidade da governança digital depende da capacidade de organizar critérios claros para coleta, tratamento e uso de dados, reduzindo efeitos adversos da mediação algorítmica e fortalecendo ambientes digitais mais confiáveis. Como limite, reconhece-se que o estudo possui natureza teórico-bibliográfica, sem incorporar investigação empírica de campo. Pesquisas futuras poderão aprofundar a análise de práticas organizacionais de governança de dados e de mecanismos institucionais de accountability em contextos específicos. Em ambientes digitais marcados por automação, plataformas e tratamento intensivo de informações, transparência, controle e responsabilização deixaram de ser atributos acessórios e passaram a constituir critérios centrais de legitimidade tecnológica.

REFERÊNCIAS

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: 29 mar. 2026.

BRASIL. Emenda Constitucional n.º 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os **direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.** Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 29 mar. 2026.

BRASIL. Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 29 mar. 2026.

BRASIL. Lei n.º 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: 30 mar. 2026.

CGI.br. **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2024.** São Paulo: Comitê Gestor da Internet no Brasil, 2024. Disponível em: https://www.cgi.br/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-domicilios-brasileiros-tic-domicilios-2024/. Acesso em: 30 mar. 2026.

CAPURRO, R. **Information ethics: a position paper. The International Review of Information Ethics, Edmonton,** v. 1, p. 1-7, jun. 2004. DOI: 10.29173/irie269. Disponível em: https://informationethics.ca/index.php/irie/article/view/269. Acesso em: 29 mar. 2026.

DONEDA, D. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados.** 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

FLORIDI, L. **The ethics of information.** Oxford: Oxford University Press, 2013. Disponível em: https://global.oup.com/academic/product/the-ethics-of-information-9780199641321. Acesso em: 29 mar. 2026.

GIL, A. C. **Métodos e técnicas de pesquisa social.** 7. ed. São Paulo: Atlas, 2019. Disponível em: https://www.grupogen.com.br/metodos-e-tecnicas-de-pesquisa-social/. Acesso em: 29 mar. 2026.

MENDES, L. S.; FONSECA, G. C. S. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. Revista Estudos Institucionais, Rio de Janeiro, v. 6, n. 2, p. 507-533, maio/ago. 2020. DOI: 10.21783/rei.v6i2.521. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/521. Acesso em: 30 mar. 2026.

MINAYO, M. C. S. **O desafio do conhecimento: pesquisa qualitativa em saúde.** 14. ed. São Paulo: Hucitec, 2014. Disponível em: https://lojahucitec.com.br/produto/maria-cecilia-de-souza-minayo-o-desafio-do-conhe cimento-pesquisa-qualitativa-em-saude/. Acesso em: 30 mar. 2026.

OECD. **Recommendation of the Council on Artificial Intelligence.** Paris: OECD, 2024. Disponível em: https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449. Acesso em: 30 mar. 2026.

ROSSETTI, Regina; ANGELUCI, Alan. **Ética algorítmica: questões e desafios éticos do avanço tecnológico da sociedade da informação.** Galáxia (São Paulo), São Paulo, n. 46, p. 1-18, 2021. Disponível em: https://revistas.pucsp.br/index.php/galaxia/article/view/50301. Acesso em: 29 mar. 2026.

SEVERINO, A. J. **Metodologia do trabalho científico.** 24. ed. São Paulo: Cortez, 2017.

UNESCO. **Recomendação sobre a ética da inteligência artificial.** Paris: UNESCO, 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000381137_por. Acesso em: 30 mar. 2026.

ZUBOFF, S. **The age of surveillance capitalism: the fight for a human future at the new frontier of power.** New York: PublicAffairs, 2019. Disponível em: https://www.hbs.edu/faculty/Pages/item.aspx?num=56791. Acesso em: 30 mar. 2026.