**ISSN 3085-5624**

Eixo Temático 1 – Produção, Mediação e Gestão da Informação

# INTEGRIDADE DA INFORMAÇÃO E PROTEÇÃO DE DADOS: CONTRIBUIÇÕES DA LGPD PARA A CONSTRUÇÃO DE ECOSSISTEMAS INFORMACIONAIS CONFIÁVEIS

## *INFORMATION INTEGRITY AND DATA PROTECTION: CONTRIBUTIONS OF THE LGPD TO THE CONSTRUCTION OF RELIABLE INFORMATION ECOSYSTEMS*

**João Rafael Ribeiro Araújo** – Universidade Federal de Alagoas (UFAL), *joaorafael.raraujo@gmail.com,* https://orcid.org/0009-0007-8793-8112

**Edivanio Duarte de Souza** – Universidade Federal de Alagoas (UFAL), *edivanio.duarte@ichca.ufal.br,* https://orcid.org/0000-0002-7461-828X

**Modalidade: Trabalho Completo**

**Resumo**: Tomando como base os dilemas da era digital, discute possibilidades de contribuição da Lei Geral de Proteção de Dados com a promoção da integridade da informação e a construção de ecossistemas informacionais confiáveis. A pesquisa possui natureza explorativa, abordagem qualitativa e orientação interdisciplinar, utilizando-se de levantamentos bibliográfico-documentais. Os resultados indicam que os princípios da legislação estudada dialogam diretamente com diretrizes internacionais voltadas à integridade da informação, sobretudo as indicadas pela Organização das Nações Unidas. Considera-se que a aplicação da referida legislação tem o potencial de favorecer práticas organizacionais éticas e inclusivas, fortalecendo ambientes digitais mais confiáveis e socialmente responsáveis.

**Palavras-chave:** proteção de dados; integridade da informação; Lei Geral de Proteção de Dados.

***Abstract**: Taking the dilemmas of the digital era as a basis, it discusses possibilities for the contribution of the General Data Protection Law to the promotion of information integrity and the construction of reliable information ecosystems. The research has an exploratory nature, qualitative approach and interdisciplinary orientation, using bibliographic-documentary surveys. The results indicate that the principles of the legislation studied dialogue directly with international guidelines aimed at the integrity of information, especially those indicated by the United Nations. It is considered that the application of said legislation has the potential to favor ethical and inclusive organizational practices, strengthening more reliable and socially responsible digital environments.*

***Keywords**: data protection; information integrity; General Data Protection Law*.

## 1 INTRODUÇÃO

A transformação digital intensificou a circulação de informações em larga escala, ampliando as possibilidades de acesso e de compartilhamento de dados, mas também expondo indivíduos, instituições e sociedades a riscos relacionados à desinformação, à violação de privacidade e à perda de confiança nas fontes e nos fluxos informacionais.

Diante desse cenário, emergem debates sobre a necessidade de estruturas normativas, técnicas e conceituais que assegurem a confiabilidade das informações que permeiam os ecossistemas digitais.

O conceito de integridade da informação tem sido cada vez mais discutido, especialmente em organismos internacionais e no campo da governança da informação, mas envolve ainda um campo conceitual em construção, com múltiplas abordagens e sem um consenso consolidado na literatura científica. De modo geral, é compreendido como a preservação da precisão, da consistência e da confiabilidade da informação. Esse tipo de integridade é apontado como um elemento estratégico para o enfrentamento da desordem da informação e para a garantia de ecossistemas informacionais saudáveis, capazes de sustentar práticas democráticas, cidadania e tomada de decisão fundamentada (ONU, 2023).

A promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil, em 2018, representa um marco legal que deve ser levado em consideração nesse debate (Brasil, 2018). Além de regulamentar o tratamento de dados pessoais, esse dispositivo legal estabelece princípios e garantias fundamentais que, ao serem observados, tem o potencial de fortalecer a integridade da informação e promover a construção de ecossistemas baseados na confiança, na transparência e na segurança. A lei ganhou ainda mais força e notoriedade quando a Emenda Constitucional nº 115/2022 (Brasil, 2022) elevou a proteção de dados ao patamar de direito fundamental, conferindo-lhe o mais alto nível hierárquico no ordenamento jurídico brasileiro (Tavares, 2023).

Essas e outras ações realizadas no horizonte do enfrentamento de problemas contemporâneos complexos, tais como desinformação, expropriação de dados, guerras de narrativas, negacionismo, notícias falsas e redes de ódio (Bezerra, 2024), evidenciam que o Estado e seus diversos entes vêm atuando, em várias frentes, no sentido de dar melhores condições para a promoção da segurança, em diversos setores, com destaque para o estabelecimento de um arcabouço jurídico que protejam direitos fundamentais. Com efeito, ao adotar uma abordagem mais crítico-hermenêutica, cabe questionar: em que bases da LGPD podem contribuir com a promoção da integralidade e a confiabilidade da informação?

Diante disso, esta comunicação tem como objetivo analisar possibilidades de contribuição da LGPD com a promoção da integridade da informação e a construção de ecossistemas informacionais confiáveis, a partir de uma abordagem teórico-conceitual que

articula os fundamentos da integridade e os princípios da proteção, nesse domínio de estudo no campo da Ciência da Informação.

A relevância desta investigação está na articulação entre duas dimensões críticas da sociedade digital contemporânea, descritas por Bezerra (2024), quem implicam direto na preocupação com a integridade da informação e a proteção de dados, e com a contribuição que essa relação pode oferecer para o fortalecimento da cidadania informacional e das políticas públicas voltadas ao tratamento ético da informação. O escopo do trabalho está centrado na análise conceitual dessas categorias, com foco nos dispositivos e nos princípios da LGPD, não se detendo, neste momento, a estudos empíricos de aplicação normativa, mas a reflexão teórica situada no campo da Ciência da Informação.

## 2 PROCEDIMENTOS METODOLÓGICOS

A presente pesquisa possui natureza exploratória qualitativa, com abordagem e orientação interdisciplinar, situando-se na interface entre a Ciência da Informação e o Direito. O método adotado foi o bibliográfico-documental, com base na análise crítica de fontes técnico-científicas, tais como artigos científicos, capítulos de livros, livros, legislações nacionais e recomendações nacionais e internacionais, relacionados à proteção de dados pessoais e à integridade da informação. Essas fontes foram selecionadas com base em sua relevância teórica, atualidade e pertinência temática. Com efeito, a coleta de dados consistiu na identificação e na análise sistemática dessas produções, com foco nos princípios da LGPD e nas recomendações de organismos nacionais e internacionais para a promoção da integridade da informação.

A análise centrou-se na identificação das possíveis conexões entre os fundamentos da integridade informacional e os princípios e dispositivos previstos na LGPD, investigando de que modo esses elementos podem, em maior ou menor medida, relacionar e promover ecossistemas informacionais mais seguros, transparentes e justos.

Trata-se, portanto, de uma pesquisa propositiva e teórico-analítica, que, embora não utilize estudo de caso empírico, apresenta hipóteses fundamentadas na literatura. Ao adotar uma perspectiva interdisciplinar, a pesquisa visa colaborar com a consolidação de referenciais teórico-metodológicos críticos e integrados para o enfrentamento dos desafios

contemporâneos que envolvem a confiabilidade das informações, a proteção de dados pessoais e a sustentabilidade dos ecossistemas digitais. Nesse sentido, o trabalho se encontra estruturado em seis seções textuais, incluindo a introdução, as reflexões e as discussões teórico-conceituais, e as considerações finais, além da seção das referências.

## 3 FUNDAMENTOS, PRINCÍPIOS E FINALIDADE DA INTEGRIDADE DA INFORMAÇÃO

A integridade da informação, embora comumente associada ao campo corporativo e à segurança da informação, vem sendo cada vez mais discutida em contextos sociais, políticos e institucionais mais amplos. Originalmente, esse conceito estava vinculado à proteção dos dados organizacionais e à confiabilidade dos sistemas informacionais internos. No entanto, atualmente, ultrapassa os limites técnicos e institucionais, abrangendo aspectos fundamentais para a vida democrática, como a veracidade, a completude e a coerência das informações que circulam na sociedade, especialmente no ambiente digital (PNUD, 2022; ONU, 2023).

Nesse sentido, a integridade da informação tem sido entendida como condição essencial para a construção de ecossistemas informacionais confiáveis. Isso implica que os cidadãos tenham acesso a dados equilibrados, contextualizados e verificáveis, capazes de subsidiar a tomada de decisões e o exercício pleno da cidadania. A Organização das Nações Unidas (ONU, 2023) reforça essa concepção ao definir integridade da informação como a soma da precisão, coerência e confiabilidade das informações disponíveis. Essa abordagem também é sustentada por Araújo (2024a), ao enfatizar que o acesso a informações confiáveis é um pilar essencial das democracias contemporâneas.

O relatório da *World Leadership Alliance – Club de Madrid (2018)* representa um marco importante no processo de adaptação do conceito ao campo das políticas públicas e da governança informacional. Produzido a partir de uma mesa redonda sobre governança global e integridade da informação, o documento propõe compreender a integridade não apenas como ausência de desinformação, mas como resultado de ações proativas voltadas à construção de um ecossistema saudável de informação. Esta análise é feita por Araújo (2024b), que também ressalta que o foco atual da integridade da informação deve ir além do combate à desinformação, de modo a deslocar o eixo do debate para uma perspectiva

positiva, centrada na proposição de práticas, normas e estratégias que promovam ambientes informacionais íntegros.

A ONU ([2024]) aprofunda essa discussão ao apresentar cinco princípios orientadores globais da integridade da informação:

1. **confiança e resiliência social**, essenciais para garantir que as sociedades possam acreditar ainda mais nas instituições e resistir a perturbações e a manipulações informacionais, inclusive aquelas impulsionadas por tecnologias como a inteligência artificial generativa;
2. **incentivos saudáveis**, que visam repensar os modelos de monetização de conteúdo que afetam negativamente o ecossistema informacional, sobretudo, com práticas de manipulação algorítmica;
3. **capacitação pública**, que diz respeito ao fortalecimento da autonomia dos indivíduos na gestão de suas experiências informacionais;
4. **mídia livre, independente e plural**, indispensável para o fortalecimento democrático e o acesso diversificado a fontes confiáveis; e
5. **transparência e pesquisa**, orientada à promoção de acesso a dados e à compreensão dos fluxos de informação, inclusive nas plataformas tecnológicas.

A ONU (2024) ainda oferece recomendações práticas direcionadas a diversos setores sociais, incluindo sociedade civil, setor público e setor privado. Entre essas recomendações, destacam-se ações voltadas à promoção da **segurança dos dados**, da **transparência**, do **acesso à informação**, da **privacidade** e da **proteção de grupos vulneráveis**, como crianças e minorias. No que se refere, especificamente, às empresas de tecnologia, que lidam com grandes volumes de dados e operam plataformas de ampla influência social, a ONU destaca que os usuários devem ter controle sobre seus dados e que as informações devem ser tratadas/utilizadas com responsabilidade. Dentre as principais recomendações, para fins de análise do presente objeto de estudo, é importante destacar:

- **integrar segurança e privacidade desde a concepção de projetos e processos**: políticas robustas devem ser incorporadas em todo o ciclo de vida dos produtos e serviços, da concepção à desativação, aplicando-se tanto à mídia gerada por humanos quanto por sistemas de inteligência artificial;

- **proteger crianças**: adotar medidas como verificação de idade, controle parental e mecanismos de denúncia específicos para garantir os direitos das crianças e combater abusos e exploração sexual infantil potencializados pelo uso da tecnologia;
- **alocar recursos internos suficientes e contínuos** para confiança e segurança, em níveis proporcionais aos riscos envolvidos;
- **comunicar políticas de forma clara e acessível**, inclusive para públicos vulneráveis, como crianças, detalhando normas comunitárias, termos de uso e regras sobre conteúdo político;
- **garantir a privacidade** dos usuários em todos os processos de coleta, armazenamento, compartilhamento e venda de dados, assegurando acesso a informações claras sobre o tratamento dos dados pessoais, inclusive em decisões algorítmicas; e
- **estabelecer mecanismos robustos de denúncia e reparação**, com canais seguros e acessíveis para usuários e não usuários, incluindo medidas específicas para grupos marginalizados e sistemas para evitar o uso abusivo dessas ferramentas.

A finalidade da integridade da informação, portanto, é promover um ambiente informacional equilibrado, justo e acessível, em que os direitos à informação e à privacidade sejam garantidos de forma integrada. Conforme destaca a ONU (2024), o fortalecimento da integridade da informação está diretamente vinculado à consecução dos Objetivos de Desenvolvimento Sustentável (ODS), pois ecossistemas informacionais degradados afetam desproporcionalmente os grupos vulnerabilizados e enfraquecem os esforços globais por justiça social, igualdade e sustentabilidade. Medidas voltadas à proteção de dados, à segurança digital, à transparência e à inclusão tornam-se, nesse contexto, componentes estruturantes de uma estratégia global para garantir a integridade da informação e fortalecer as bases de uma sociedade democrática e confiável.

## 4 PRINCÍPIOS DA PROTEÇÃO DE DADOS PESSOAIS À LUZ DA LGPD

A Lei nº 13.709/2018, conhecida como LGPD, foi criada em um cenário de crescente uso e circulação de dados pelas instituições públicas e privadas, como forma de

regulamentar e trazer segurança jurídica ao tratamento de dados pessoais no Brasil. Inspirada no *General Data Protection Regulation* (GDPR), a legislação brasileira passou a estabelecer princípios, direitos e deveres voltados à proteção dos indivíduos diante desta nova economia dos dados, promovendo equilíbrio entre inovação tecnológica, desenvolvimento econômico e respeito aos direitos fundamentais (Ferreira; Pinheiro; Marques, 2021).

Com a Emenda Constitucional nº 115/2022, conforme esclarece Moraes (2024) a proteção de dados pessoais foi elevada a direito fundamental, garantindo ao tema o mais alto nível hierárquico dentro do ordenamento jurídico brasileiro. Essa mudança reforça o caráter essencial da privacidade e da proteção dos dados para o exercício pleno da cidadania na era digital.

A legislação estabelece dez princípios norteadores que devem ser observados por todos os agentes de tratamento, públicos ou privados, na medida em que funcionam como pilares para assegurar que o tratamento de dados seja feito com ética, responsabilidade e respeito aos direitos dos titulares, sendo também instrumentos que fortalecem a integridade e a confiança nos ambientes informacionais físicos e digitais.

O **princípio da finalidade** determina que o tratamento de dados deve sempre atender a propósitos legítimos, específicos e informados ao titular; sendo assim, as instituições acabam sofrendo limitações na utilização destes dados para propósitos incompatíveis com a finalidade inicialmente indicada ao usuário (Autoridade Nacional de Proteção de Dados, 2023).

O **princípio da adequação**, por sua vez, exige que o uso dos dados seja compatível com a finalidade informada e com o contexto do tratamento realizado. O **princípio da necessidade**, apesar de ser parecido com o da adequação, possui peculiaridades em sua hermenêutica, já que obriga que sejam tratados apenas os dados mínimos indispensáveis à realização da finalidade pretendida, promovendo o uso proporcional e limitado das informações (Autoridade Nacional de Proteção de Dados, 2023). No princípio da necessidade, ainda que o dado seja compatível, sua coleta e sua utilização devem ser evitadas se outros dados já coletados sejam suficientes para alcançar a finalidade pretendida.

O quarto princípio previsto na lei é o do **livre acesso**, que assegura ao titular o direito de consultar, de forma facilitada e gratuita, todas as informações relativas ao tratamento de seus dados pessoais. Isso inclui o conhecimento sobre a existência do tratamento, as finalidades, os responsáveis, o tempo de retenção dos dados e demais elementos que compõem o ciclo de vida da informação. Tal princípio é essencial para garantir a autonomia informativa do cidadão, além de viabilizar o controle social sobre instituições que tratam dados.

Já o **princípio da segurança** determina que os agentes de tratamento devem adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Essas medidas envolvem tanto a proteção física quanto digital das informações, com políticas ativas de gestão de riscos, auditorias e boas práticas de governança (Autoridade Nacional de Proteção de Dados, 2021).

O **princípio da transparência**, por seu turno, obriga os agentes a fornecerem informações claras, precisas e acessíveis aos titulares sobre o tratamento de seus dados; estas ações de transparência devem ser de forma ativa, isto é, independente de provocação ou solicitação dos titulares. Além de ser um fundamento da própria LGPD, a transparência é um requisito essencial para que os indivíduos possam exercer plenamente seus direitos e, portanto, para que haja integridade nos fluxos informacionais entre o Estado, empresas e cidadãos (Autoridade Nacional de Proteção de Dados, 2023).

Em relação ao **princípio da qualidade dos dados**, há um claro reforço à obrigação de manter as informações exatas, atualizadas, pertinentes e verdadeiras, de modo a evitar distorções, desinformação ou prejuízos aos titulares. Já o **princípio da prevenção** impõe uma postura ativa dos agentes de tratamento para evitar danos, por meio da antecipação de riscos e da adoção de práticas de segurança da informação.

Destaca-se também o **princípio da não discriminação**, que proíbe o tratamento de dados para fins discriminatórios, ilícitos ou abusivos. Isso envolve, por exemplo, o uso indevido de dados sensíveis, como informações sobre raça, religião, orientação sexual, saúde ou opiniões políticas, o que poderia gerar exclusão social, discriminação automatizada e violações de direitos humanos.

O último princípio explícito no artigo 6º é o da **responsabilização e prestação de contas**, pautado na exigência de que os agentes de tratamento devem comprovar adoção de medidas eficazes para garantir o cumprimento da LGPD, inclusive mantendo registros e relatórios que demonstrem essa conformidade. É um princípio que fortalece a governança institucional e a confiança entre os diferentes atores que operam em ecossistemas informacionais.

Nesse contexto, é igualmente relevante destacar o princípio do **melhor interesse da criança e do adolescente**, previsto no artigo 14 da LGPD, o qual estabelece que o tratamento de dados pessoais de menores deve ser realizado com base em seu melhor interesse. A norma determina, entre outros aspectos, que o consentimento para o tratamento de dados de crianças seja dado por, pelo menos, um dos pais ou responsável legal e que as informações prestadas aos titulares e seus responsáveis sejam claras, acessíveis e adaptadas às características cognitivas e sensoriais do público infantojuvenil (Autoridade Nacional de Proteção de Dados, 2024b). Tal princípio reforça a necessidade de proteger sujeitos em condição peculiar de desenvolvimento diante dos riscos informacionais, evidenciando a função protetiva dessa norma frente às desigualdades digitais e aos potenciais danos associados ao uso indevido de dados, especialmente em ambientes altamente automatizados ou publicitários.

Ainda que não esteja expressamente elencado no artigo 6º, a LGPD **reforça o princípio implícito do *privacy by design*** em seu artigo 46, §2º (Brasil, 2018). Esse princípio orienta que a privacidade e a proteção de dados devem ser incorporadas desde a concepção de qualquer projeto, produto ou serviço que envolva o tratamento de dados pessoais. Ou seja, medidas de segurança e de respeito à privacidade não devem ser pensadas como soluções corretivas ou acessórios operacionais, mas sim como elementos estruturantes e contínuos de todo o ciclo de tratamento. Segundo Oliveira (2021), essa abordagem favorece a construção de uma cultura organizacional mais preventiva, transparente e ética — elementos indispensáveis à integridade da informação.

Outro elemento fundamental previsto na LGPD é a figura do **Encarregado pelo Tratamento de Dados Pessoais**, também conhecido como *Data Protection Officer* (DPO). De acordo com o artigo 41 da lei, as instituições devem indicar esse profissional e tornar públicas sua identidade e informações de contato, para viabilizar sua comunicação com os

titulares, agentes de tratamento e/ou com a Autoridade Nacional de Proteção de Dados (ANPD)[1]. Cumpre ressaltar que a ANPD ratificou o texto legal ao afirmar que o DPO contribui decisivamente para a implementação efetiva dos princípios daquela normativa, servindo como elo entre a teoria normativa e a prática institucional no cuidado com os dados pessoais e a integridade dos fluxos informacionais (Autoridade Nacional de Proteção de Dados, 2024a).

A compreensão e a aplicação consistente desses princípios criam condições para o fortalecimento de ecossistemas informacionais mais íntegros, confiáveis e seguros. Como será explorado mais à frente, esses fundamentos são especialmente relevantes na construção de ambientes em que o fluxo de dados ocorre com responsabilidade, equidade e transparência, favorecendo o desenvolvimento de políticas informacionais centradas na dignidade da pessoa humana e na confiabilidade das informações.

## 5 APLICAÇÃO DA LGPD NA PROMOÇÃO DE ECOSSISTEMAS INFORMACIONAIS CONFIÁVEIS

A construção de ecossistemas informacionais confiáveis exige mais do que infraestrutura tecnológica robusta, na medida em que pressupõe a implementação de princípios éticos, jurídicos e operacionais que garantam a proteção de dados, a transparência nas práticas informacionais e o respeito à privacidade individual. Como discutido acima, a integridade da informação e os princípios norteadores da LGPD formam os pilares dessa construção, atuando como mecanismos preventivos e normativos que orientam a gestão responsável dos dados. Aquela norma, neste contexto, constitui um marco regulatório com grande potencial de promoção de ambientes digitais confiáveis.

No que tange à proteção de dados pessoais, a LGPD carrega em seu conteúdo principiológico e operacional uma série de diretrizes que, quando colocadas em prática, têm o potencial de fomentar ecossistemas que respeitam não apenas a privacidade, mas também a integridade, a ética e a segurança da informação. É justamente esse compromisso com a confiabilidade informacional que é reforçado por recomendações internacionais, como as emitidas pela ONU, em favor de uma governança digital ética, transparente e inclusiva, que promova a integridade da informação. A sinergia entre as normas nacionais e

[1] Nos termos do artigo 5º, XIX da LGPD, a ANPD é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

os padrões globais amplia o alcance das garantias aos cidadãos e fortalece os pilares dos ecossistemas digitais confiáveis.

Nesse sentido, observa-se, por exemplo, uma forte convergência entre o princípio da **transparência**, previsto na LGPD, e o princípio da **confiança e resiliência social**, recomendado pela ONU. Ambos destacam a importância de canais institucionais claros, acessíveis e confiáveis, por meio dos quais os cidadãos possam acessar informações precisas sobre o tratamento de dados. Essa transparência fortalece o papel das instituições públicas e privadas como fontes legítimas de informação, especialmente em contextos marcados por desinformação e notícias falsas. Ao garantirem o acesso à origem e – em certa medida – ao fluxo dos dados, essas instituições não apenas promovem a integridade informacional, mas também consolidam sua credibilidade social.

Outro ponto de interseção relevante se estabelece entre o princípio da **finalidade**, da LGPD, e a diretriz da ONU que trata da criação de **incentivos saudáveis**. A ONU (2024) recomenda que empresas e plataformas digitais avaliem criticamente suas estratégias de conteúdo e de publicidade, de modo a evitar práticas manipulativas ou exploratórias, que correspondem, em grande medida ao cerne das questões éticas em torno da informação apontadas por Bezerra (2024), dentre as quais se destacam expropriação e alienação de dados. A LGPD, no oriente do enfrentamento desses elementos críticos, exige que o tratamento de dados se restrinja – ou ao menos seja compatível – às finalidades informadas no momento da coleta. O desvio dessas finalidades, como ocorre quando dados são compartilhados com terceiros para publicidade direcionada sem o consentimento do titular (Bezerra, 2024), compromete a integridade do ecossistema e a confiança do usuário. A aplicação criteriosa do princípio da finalidade, portanto, contribui para conter abusos e estabelecer práticas mais justas e éticas.

Embora o princípio da **capacitação pública**, indicado pela ONU (2024), se volte principalmente às organizações privadas, a LGPD também incorpora esse compromisso. O artigo 55-J atribui à ANPD a responsabilidade de fomentar o conhecimento público sobre proteção de dados, medidas de segurança e direitos dos titulares. Trata-se de uma ação educativa que fortalece a autonomia informacional dos cidadãos e promove uma cultura de proteção de dados, elemento indispensável para a resiliência e o amadurecimento dos ecossistemas digitais.

Destaca-se, ainda, a convergência entre as recomendações da ONU (2024) sobre **a integração de segurança e a privacidade desde a concepção de projetos** e **os princípios do *privacy by design*** e da **prevenção**, presentes na LGPD. Conforme dispõe o artigo 46, §2º dessa Lei, o tratamento de dados deve observar medidas proativas de segurança desde a origem dos sistemas, o que inclui o planejamento técnico e organizacional para evitar riscos antes mesmo de sua materialização. Essa abordagem preventiva está em consonância com os princípios da integridade da informação, pois evita vulnerabilidades que poderiam comprometer a veracidade, a confiabilidade e a segurança dos dados tratados.

No que se refere à **proteção de dados de crianças e adolescentes**, as diretrizes da ONU (2024) encontram respaldo direto no artigo 14 da LGPD. A norma estabelece que o tratamento de dados de menores deve observar o seu melhor interesse, exigir consentimento específico dos responsáveis e garantir que as informações sejam fornecidas de forma clara e acessível ao menor e aos responsáveis, inclusive com a utilização de recursos audiovisuais necessários. Tal preocupação com a linguagem acessível e com o consentimento informado reforça a ideia de uma governança informacional ética e inclusiva, particularmente sensível às especificidades de públicos vulneráveis.

A LGPD também compartilha com a ONU (2024) a premissa de que a **alocação de recursos internos contínuos** é condição fundamental para garantir segurança e confiança no tratamento de dados. Os princípios da **segurança** e da **prevenção**, previstos na lei, exigem das organizações investimentos permanentes em tecnologia, gestão de riscos e capacitação, de modo a evitar falhas e vazamentos. Como pontuam Almeida e Soares (2022), o novo marco legal impõe às instituições públicas e privadas a responsabilidade de desenvolver programas internos alinhados às exigências legais, com políticas bem estruturadas, equipes treinadas e mecanismos de monitoramento contínuo.

A preocupação da ONU (2024) com a **comunicação clara e acessível das políticas de privacidade** também se reflete na LGPD, especialmente no princípio da **transparência** e nas disposições sobre os direitos dos titulares. A clareza na apresentação das informações é essencial para garantir o livre acesso do cidadão às práticas de tratamento de dados e, consequentemente, para reforçar a integridade informacional. Neste sentido, Kohls, Dutra e Welter (2022) destacam que a conformidade com a LGPD não apenas mitiga riscos jurídicos,

mas também agrega valor reputacional às organizações, fortalece a confiança dos usuários e amplia a competitividade no mercado digital.

Nesse panorama, é importante ainda destacar a relação entre a LGPD e a diretriz da ONU (2024) que prevê a garantia da **privacidade dos usuários durante todo o ciclo de tratamento de dados**, inclusive em decisões automatizadas, um dos principais diletas éticos da era digital apontados por Bezerra (2024), sobretudo, no contexto das mediações algorítmicas. O artigo 20 da LGPD assegura ao titular o direito de solicitar a revisão de decisões tomadas com base exclusivamente em tratamento automatizado, como nos casos de análise de crédito ou perfis de consumo. A norma também obriga as instituições a explicarem, quando solicitadas, os critérios utilizados nesses processos, reforçando o compromisso com a ética algorítmica e a transparência das decisões digitais.

Essa preocupação da LGPD com as decisões automatizadas é especialmente relevante diante do risco de reprodução de vieses algorítmicos discriminatórios, frequentemente embutidos em sistemas automatizados de decisão. Essas tendências, muitas vezes, derivadas de conjuntos de dados incompletos ou historicamente enviesados, podem perpetuar desigualdades e injustiças, impactando diretamente direitos fundamentais, como o acesso a crédito, emprego ou serviços públicos (Bezerra, 2024, Sainz; Gabardo; Ongaratto, 2024). Ao prever o direito à revisão e à explicação dessas decisões, a LGPD busca mitigar tais riscos, promovendo maior equidade e integridade no tratamento automatizado de dados, o que se alinha, inclusive, com a recomendação da ONU (2024) de auditorias independentes que avaliem potencial discriminatório de inteligências artificiais.

Por fim, há um elo importante entre as recomendações da ONU (2024) quanto à necessidade de mecanismos robustos de denúncia e de reparação e o artigo 41 da LGPD, que estabelece a figura do encarregado pelo tratamento de dados pessoais. Cabe a esse profissional receber comunicações dos titulares, prestar esclarecimentos e adotar providências necessárias para fiel cumprimento da LGPD na instituição (Autoridade Nacional de Proteção de Dados, 2024a). Além disso, a própria ANPD disponibiliza canais formais de denúncia, permitindo que a sociedade civil participe ativamente da fiscalização e da correção de práticas abusivas no tratamento de dados. Essa estrutura de responsabilização e de controle social contribui decisivamente para o fortalecimento de ecossistemas informacionais confiáveis e resilientes.

Dessa forma, é possível afirmar que a aplicação da LGPD vai além da proteção individual de dados, atuando como uma engrenagem fundamental na construção de ambientes digitais íntegros, éticos e sustentáveis. Ao integrar os princípios nacionais aos padrões internacionais, como os da ONU, a legislação brasileira potencializa seus efeitos e contribui para o desenvolvimento de uma cultura informacional que valoriza a confiança, a transparência e o respeito aos direitos fundamentais.

## 6 CONSIDERAÇÕES FINAIS

A transformação digital intensificou a circulação de informações em larga escala, ampliando as possibilidades de acesso e de compartilhamento de dados, mas também expondo indivíduos, instituições e sociedades a riscos relacionados à desinformação, à violação de privacidade e à perda de confiança nas fontes e nos fluxos informacionais. Nesse contexto, tornaram-se urgentes os debates sobre a criação e o fortalecimento de estruturas normativas, técnicas e conceituais capazes de assegurar a confiabilidade das informações que circulam nos ecossistemas digitais.

Surge, então, o conceito de integridade da informação, que embora ainda esteja em processo de construção na literatura, tem chamado atenção, especialmente em organismos internacionais e no campo da governança da informação, sendo geralmente associado à preservação da precisão, da consistência e da confiabilidade dos dados. Sua promoção é considerada estratégica para enfrentar a desordem informacional e para garantir ambientes informacionais saudáveis, capazes de sustentar a cidadania, a democracia e a tomada de decisões fundamentadas.

e sentido, este estudo teve como propósito refletir sobre as possibilidades de contribuições da LGPD para a promoção da integridade da informação e para o fortalecimento de ecossistemas informacionais confiáveis. A análise apontou que os princípios e os fundamentos que norteiam a LGPD dialogam diretamente com os princípios que sustentam a integridade da informação, estabelecendo pontes com diretrizes internacionais, sobretudo aquelas emitidas pela ONU, na publicação dos Princípios Globais das Nações Unidas para a Integridade da Informação, na qual enfatiza a importância da

transparência, da segurança, da privacidade e do respeito aos direitos humanos no ambiente digital.

Ao longo das análises e discussões, ficou registrado que os princípios expressos e implícitos da LGPD — entre eles, o livre acesso, a segurança, a transparência, a não discriminação e a adoção do *privacy by design* — compõem um conjunto articulado que visa garantir o tratamento ético, confiável e responsável das informações. Com efeito, esses princípios não apenas regulam o uso dos dados pessoais, mas também contribuem para o fortalecimento de práticas organizacionais voltadas à confiança, à proteção dos usuários e à promoção da justiça informacional, especialmente no enfrentamento de desigualdades e na proteção de grupos vulneráveis.

A promoção da LGPD nos setores público e privado mostra-se, portanto, como uma estratégia para fomentar práticas que garantam o tratamento ético, seguro e transparente das informações. Ao valorizar a autodeterminação informativa e ao estabelecer diretrizes claras para o uso de dados, a referida legislação contribui diretamente para a construção de ambientes digitais mais íntegros, inclusivos e atentos às vulnerabilidades sociais.

Agora, resta problematizar cada vez mais em que medida é possível se efetivar essa autodeterminação, pelo menos, em parte da população brasileira, em um mundo cada vez mais mediado por fortes e poderosas relações algorítmicas. Aqui, resta claro que a presente discussão não se propôs a esgotar o tema, mas a abrir margem para novas investigações. Uma possível linha de pesquisa futura diz respeito à análise de como a implementação de programas de conformidade à LGPD pode influenciar diretamente a integridade da informação nas organizações, impactando seus processos internos, suas estruturas de governança e suas práticas informacionais de modo mais amplo e profundo.

## REFERÊNCIAS

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 27, n. 3, p. 26-45, jul./set 2022. Disponível em: https://periodicos.ufmg.br/index.php/pci/issue/view/1929. Acesso em: 29 ago. 2025.

ARAÚJO, Carlos Alberto Ávila. Integridade da informação: nova problemática para a mediação da informação. **Infor**, Montevideo, v. 29, n. 2, dez. 2024a. Disponível em: http://www.scielo.edu.uy/scielo.php?script=sci_arttext&pid=S2301-13782024000201206&lng=es&nrm=iso&tlng=pt#B28. Acesso em: 28 jul. 2025.

ARAÚJO, Carlos Alberto Ávila. Integridade da informação: um novo conceito para o estudo da desinformação. **Revista Comunicação Midiática**, Bauru, SP, v. 19, n. 1, p. 207–226, 2024b. DOI: 10.5016/gpkkyf59. Disponível em: https://www2.faac.unesp.br/comunicacaomidiatica/index.php/CM/article/view/614. Acesso em: 28 jul. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia orientativo**: atuação do encarregado pelo tratamento de dados pessoais. Brasília: [*s.n.*], 2024a. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_da_atuacao_do_encarregado_anpd.pdf/view. Acesso em: 29 jul. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte**. Brasília: [*s.n.*], 2021. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-sobre-seguranca-da-informacao-para-agentes-de-tratamento-de-pequeno-porte. Acesso em: 29 jul. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Tratamento de dados pessoais pelo Poder Público**. Brasília: [*s.n.*], 2023. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/materiais-educativos. Acesso em: 29 jul. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Nota Técnica nº 50/2024FIS/CGF/ANPD. **Tratamentos de dados pessoais de crianças e adolescentes pela rede social TikTok**, Brasília: [*s.n.*], nov. 2024b. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/documentos_tecnicos. Acesso em: 29 jul. 2025.

BEZERRA, Arthur Coelho. **Miséria da informação:** dilemas éticos da era digital. Rio de Janeiro: Garamond, 2024.

BRASIL. **Emenda Constitucional nº 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, 10 de fevereiro de 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 11 jul. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 jul. 2025.

FERREIRA, Daniela Assis Alves; PINHEIRO, Marta Macedo Kerr; MARQUES, Rodrigo Moreno. Privacidade e proteção de dados pessoais: perspectiva histórica. **InCID**: Revista de Ciência da

Informação e Documentação, Ribeirão Preto, v. 12, n. 2, p. 151-172, 2021. Disponível em: https://revistas.usp.br/incid/article/view/179778. Acesso em: 28 jul. 2025.

KOHLS, Cleize; DUTRA, Luiz Henrique; WELTER, Sandro. **LGPD**: da teoria à implementação nas empresas. 2. ed. São Paulo: Rideel, 2022.

MORAES, Alexandre de. **Direito Constitucional**. 40. ed. rev. Atual. Barueri [SP]: Atlas, 2024.

OLIVEIRA, R. **LGPD**: Como evitar as avaliações administrativas. Rio de Janeiro: Expressa, 2021.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Informe de política para a nossa agenda comum**: integridade da informação nas plataformas digitais. [*S. l.*]: ONU, out. 2023. Disponível em: https://brasil.un.org/pt-br/249996-integridade-da-informa%C3%A7%C3%A3o-nas-plataformas-digitais-informe-do-secret%C3%A1rio-geral-da-onu. Acesso em: 26 jul. 2025.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Princípios globais para a integridade da informação**: Recomendações para ação de múltiplas partes interessadas. [*S. l.*]: ONU, jun. [2024]. Disponível em: https://brasil.un.org/pt-br/274644-princ%C3%ADpios-globais-para-integridade-da-informa%C3%A7%C3%A3o. Acesso em: 26 jul. 2025.

PROGRAMA DE LAS NACIONES UNIDAS PARA EL DESARROLLO (PNUD). **Integridad de la información**: allanar el camino a la verdad, la resiliencia y la confianza. Nueva York, fev. 2022. Disponível em: https://www.undp.org/publications/information-integrity-forging-pathway-truth-resilience-and-trust. Acesso em: 26 jul. 2025.

SAINZ, Nilton; GABARDO, Emerson; ONGARATTO, Natália. Discriminação algorítmica no Brasil: uma análise da pesquisa jurídica e suas perspectivas para a compreensão do fenômeno. **RDP**: Revista Direito Público, Brasília, v. 21, n. 110, p. 258-289, abr./jun. 2024. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/7295. Acesso em: 26 jul. 2025.

TAVARES, André Ramos. **Curso de Direito Constitucional**. 21. ed. São Paulo: SaraivaJur, 2023.

WORLD LEADERSHIP ALLIANCE – CLUB DE MADRID. **Protecting Information Integrity:** National and International Policy Options. Report of the Roundtable on Global Governance for Information Integrity held in Riga (Latvia) on 27 September 2018. Riga: Ministry of Foreign Affairs, 2018. Disponível em: https://clubmadrid.org/wp-content/uploads/2019/03/Protecting-Information-Integrity-WEB.pdf. Acesso em: 26 jul. 2025.

**NOTA**

[1] Este trabalho foi realizado no escopo das atividades do Projeto “Socialização do Método do Estudo Imanente em Informação”, chamada CNPq/MCTI Nº 10/2023, sob a supervisão do Professor Doutor Edivanio Duarte de Souza.