

# **IX ENCONTRO VIRTUAL DO CONPEDI**

**DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS  
IV**

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

#### **Diretoria - CONPEDI**

**Presidente** - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - FMU - São Paulo

**Diretor Executivo** - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

**Vice-presidente Norte** - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

**Vice-presidente Centro-Oeste** - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

**Vice-presidente Sul** - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

**Vice-presidente Sudeste** - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

**Vice-presidente Nordeste** - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

**Representante Discente:** Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

#### **Conselho Fiscal:**

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFRSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Ednilson Donisete Machado - UNIVEM/UENP - São Paulo

#### **Secretarias**

#### **Relações Institucionais:**

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

#### **Comunicação:**

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

#### **Relações Internacionais para o Continente Americano:**

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

#### **Relações Internacionais para os demais Continentes:**

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

#### **Educação Jurídica**

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR

Prof. Dr. Rubens Beçak - USP - SP

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - MS

#### **Eventos:**

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

#### **Comissão Especial**

Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG

Prof. Dr. Rogério Borba - UNIFACVEST - SC

D597

Direito, governança e novas tecnologias IV [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Irineu Francisco Barreto Junior; Diogo de Almeida Viana dos Santos – Florianópolis: CONPEDI, 2026.

Inclui bibliografia

ISBN: 978-65-5274-588-0

Modo de acesso: [www.conpedi.org.br](http://www.conpedi.org.br) em publicações

Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Direito. 3. Governança e novas tecnologias. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34



## **IX ENCONTRO VIRTUAL DO CONPEDI**

### **DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS IV**

---

#### **Apresentação**

Os trabalhos que integram esta publicação foram apresentados no Grupo de Trabalho “Direito, Governança e Novas Tecnologias IV”, realizado virtualmente no dia 25 de junho de 2026, como parte da programação do IX Encontro Virtual do Conselho Nacional de Pesquisa e Pós-graduação em Direito (CONPEDI). Esta edição do evento reafirma o compromisso histórico desta sociedade científica, que há décadas promove a excelência na pesquisa jurídica, adaptando-se às novas realidades de interação digital para garantir a continuidade do diálogo acadêmico em nível nacional e internacional.

O presente Grupo de Trabalho consolidou-se como um espaço privilegiado de interlocução, destacando-se não apenas pela densidade teórica dos trabalhos expostos, mas também pelo perfil de seus participantes, composto por professores pesquisadores, doutores, mestres e alunos de pós-graduação, que trouxeram o frescor de suas investigações institucionais para o debate coletivo. A dinâmica das apresentações, conduzida em ambiente virtual, propiciou uma interação instigante entre os autores e o público, permitindo que a pesquisa jurídica fosse discutida sob o prisma da transdisciplinaridade e do enfrentamento dos desafios contemporâneos.

A temática central deste GT, focada na governança e nas novas tecnologias, reflete a inquietude necessária diante das constantes transformações da sociedade da informação. Cientes da complexidade desses fenômenos, os pesquisadores buscaram articular respostas jurídicas para uma realidade que se apresenta em fluxo permanente, onde a técnica e o Direito se entrelaçam. Nesse sentido, as discussões perpassaram por eixos fundamentais que estruturam o debate acadêmico atual, tais como:

Tecnologias Emergentes e Sociedade: A investigação sobre os impactos da cibercultura na esfera pública, o uso da tecnologia como ferramenta de persuasão e os desafios éticos impostos pela biotecnologia e pela segurança pública.

Os trabalhos selecionados para esta coletânea são o resultado de pesquisas rigorosas desenvolvidas em diversos Programas de Pós-graduação em Direito do país. Ressalte-se que todos os artigos foram submetidos a um criterioso processo de seleção, por meio do sistema de dupla avaliação cega por pares (double blind peer review), garantindo o rigor científico e a adequação temática aos propósitos deste Grupo de Trabalho.

Ao apresentar estes anais ao público, os coordenadores manifestam a expectativa de que estas reflexões contribuam efetivamente para o fortalecimento do diálogo interdisciplinar e para o avanço da ciência jurídica brasileira. O objetivo é oferecer aos leitores um panorama crítico e atualizado sobre como o Direito pode e deve mediar as relações em um mundo cada vez mais pautado pela inovação tecnológica, assegurando sempre a prevalência da dignidade humana e dos valores democráticos.

Desejamos a todos uma leitura proveitosa e inspiradora.

Os Coordenadores

Prof. Dr. Irineu Francisco Barreto Junior (Mestrado em Direito das Faculdades Metropolitanas Unidas - FMU-SP)

Prof. Dr. Diogo de Almeida Viana dos Santos (Universidade Estadual do Maranhão; Universidade CEUMA-PPG em Direito e Afirmação de Vulneráveis)

## **GOVERNANÇA DIGITAL E VIGILÂNCIA: A COMPATIBILIZAÇÃO DA LEI DE ACESSO À INFORMAÇÃO COM A LGPD**

### **DIGITAL GOVERNANCE AND SURVEILLANCE: HARMONIZING THE ACCESS TO INFORMATION LAW WITH THE GENERAL DATA PROTECTION LAW (LGPD)**

**Maurício Testoni**

#### **Resumo**

A crescente digitalização da Administração Pública e a expansão de tecnologias de vigilância e tratamento massivo de dados têm intensificado tensões entre dois regimes jurídicos fundamentais no Brasil: a Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados Pessoais (LGPD). A conjugação desses diplomas revela um desafio normativo e institucional complexo: assegurar transparência administrativa, princípio estruturante do Estado Democrático de Direito, ao mesmo tempo em que se protege a privacidade e a dignidade informacional dos cidadãos. O estudo demonstra que a compatibilização entre LAI e LGPD não depende apenas de interpretação jurídica, mas de um modelo robusto de governança digital, baseado em gestão de riscos, proporcionalidade, finalidade pública, governança algorítmica e estruturas institucionais maduras. A análise evidencia que a proteção de dados não constitui obstáculo à publicidade, mas componente essencial para evitar práticas abusivas de vigilância, especialmente em um contexto marcado pela inteligência artificial, decisões automatizadas e ampliação das capacidades estatais de tratamento de dados. Conclui-se que a harmonização entre transparência e proteção de dados é possível e necessária, desde que apoiada em práticas administrativas responsáveis, infraestrutura tecnológica adequada, supervisão regulatória e cultura organizacional orientada à integridade.

**Palavras-chave:** Governança digital, Lei de acesso à informação, Proteção de dados pessoais, Vigilância estatal, Transparência pública

#### **Abstract/Resumen/Résumé**

public purpose, algorithmic governance, and mature institutional structures. The analysis shows that data protection does not constitute an obstacle to transparency; rather, it is an essential component for preventing abusive surveillance practices, especially in a context shaped by artificial intelligence, automated decision-making, and the expansion of state capacities for data processing. It is concluded that harmonizing transparency and data protection is both possible and necessary, provided it is supported by responsible administrative practices, adequate technological infrastructure, regulatory oversight, and an organizational culture oriented toward integrity.

**Keywords/Palabras-claves/Mots-clés:** Digital governance, Access to information law, Personal data protection, State surveillance, Public transparency

## INTRODUÇÃO

A progressiva digitalização da Administração Pública e a consequente expansão das tecnologias de tratamento de dados têm produzido alterações estruturais significativas no funcionamento do Estado brasileiro. Esse processo, caracterizado pela adoção de sistemas automatizados, inteligência artificial e modelos de decisão baseados em dados, amplia a capacidade estatal de gestão e de formulação de políticas públicas. Entretanto, tal evolução gera tensões entre dois regimes jurídicos fundamentais: o dever de transparência previsto na Lei de Acesso à Informação (Lei Federal n.º 12.527/2011) e o direito fundamental à privacidade e à proteção de dados pessoais consagrado pela Lei Geral de Proteção de Dados Pessoais (Lei Federal n.º 13.709/2018).

Nesse contexto, coloca-se o problema central que orienta a presente pesquisa: de que modo compatibilizar a publicidade dos atos administrativos com a salvaguarda dos dados pessoais, especialmente quando o Estado intensifica o uso de tecnologias capazes de ampliar sua capacidade de vigilância e de análise informacional.

A literatura especializada aponta que a relação entre Poder Público e titular de dados é marcada por evidente assimetria, destacando que o Estado detém grandes volumes de informações pessoais e exerce poder de império, o que torna necessário um regime rigoroso de tratamento de dados para evitar violações de direitos fundamentais (TASSO, 2020, p. 246). A ausência de governança eficaz intensifica riscos de uso indevido, discricionariedade excessiva e incremento de práticas de vigilância incompatíveis com parâmetros democráticos.

Simultaneamente, fenômenos globais como o capitalismo de vigilância remodelam a dinâmica informacional contemporânea. Para Zuboff (2021) a coleta ubíqua de dados e sua conversão em matéria-prima para fins de predição comportamental alteram profundamente a concepção tradicional de privacidade. A proteção de dados emerge, assim, como condição essencial para o exercício de demais direitos fundamentais e para a preservação da autonomia individual.

No âmbito brasileiro, a necessidade de compatibilização entre LAI e LGPD assume relevância ampliada, pois envolve a harmonização entre a publicidade como princípio constitucional de magnitude democrática, e a proteção da dignidade informacional. As pesquisas sobre governança pública ressaltam que transparência, integridade e gestão de riscos devem ser consideradas dimensões complementares de um

mesmo sistema institucional, e não esferas conflitantes (NOHARA; GONÇALVES; ALMEIDA, 2021).

Parte-se, portanto, da hipótese de que a compatibilização normativa entre LAI e LGPD é não apenas possível, mas necessária para garantir um modelo de governança digital responsável, orientado por direitos fundamentais e pela eficiência administrativa.

## **2 Governança Digital e Transformação Administrativa**

A governança digital compreende o conjunto de estruturas, processos e mecanismos destinados a orientar o uso de tecnologias da informação pelo Estado. Trata-se de fenômeno que ultrapassa a mera informatização de procedimentos, configurando verdadeira reorganização das práticas administrativas.

Estudos recentes apontam que a incorporação de inteligência artificial, sistemas algorítmicos e modelos de decisão automatizada requer novas estruturas de responsabilização, transparência e controle, uma vez que esses instrumentos possuem potencial para gerar opacidade decisória e reforçar desigualdades informacionais. A reconfiguração da organização administrativa em ambiente digital exige, portanto, a adoção de mecanismos técnicos e jurídicos que assegurem eficiência e, simultaneamente, proteção dos titulares de dados (ORGANIZAÇÃO ADMINISTRATIVA E IA, 2022).

Nesse sentido, os princípios da LGPD (finalidade, adequação, necessidade, transparência, segurança e responsabilidade) passam a orientar o ciclo completo do tratamento de dados na Administração Pública.

Para Anna Levin (2020) o tratamento de dados pelo Estado deve sempre estar vinculado à finalidade pública e submetido ao regime jurídico administrativo, não podendo ser praticado de forma desviante ou desproporcional (LEVIN, 2020).

### **2.1 Transparência Pública e a Lei de Acesso à Informação**

A publicidade dos atos administrativos é princípio estruturante do constitucionalismo republicano. A Lei de Acesso à Informação consolidou esse entendimento ao estabelecer o acesso à informação como regra e o sigilo como exceção. A transparência é concebida como instrumento de controle social, prevenção de desvios, fortalecimento institucional e legitimação democrática.



Autores que analisam modelos de governança pública, especialmente no âmbito das empresas estatais, destacam que a transparência se relaciona diretamente à integridade e ao desempenho organizacional, constituindo requisito mínimo para a confiança pública e para o funcionamento adequado de sistemas de *compliance* (NOHARA; GONÇALVES; ALMEIDA, 2021).

Entretanto, a transparência encontra limites jurídicos quando envolve dados pessoais, pois, o Art. 31 da LAI reconhece que informações pessoais devem ter acesso restrito, salvo situações em que o interesse público prevaleça.

Essa limitação impõe a necessidade de uma interpretação sistemática com a LGPD, de modo a evitar tanto a supressão indevida de informações quanto a exposição desnecessária de dados sensíveis.

## **2.2 Proteção de Dados Pessoais como Direito Fundamental**

A LGPD introduz no Brasil um regime normativo que visa proteger a pessoa natural diante do tratamento intensivo de dados. Inspirada no GDPR europeu, a lei tem por objetivo equilibrar inovação e proteção de direitos fundamentais, garantindo previsibilidade jurídica, padronização de práticas e mitigação de riscos.

A doutrina especializada enfatiza que a lei não busca proibir o tratamento de dados, mas estabelecer parâmetros para seu uso legítimo.

Nesse sentido, para Cláudia e Bruno Finkelstein a informação passou a ser considerada ativo econômico relevante, razão pela qual sua circulação deve observar garantias mínimas de segurança, transparência e proporcionalidade. A ausência desses parâmetros expõe a sociedade ao risco de formação de “ditaduras digitais” baseadas em vigilância tecnológica e acúmulo informacional indiscriminado (FINKELSTEIN; FINKELSTEIN, 2020).

Além disso, a relação entre o cidadão e o Poder Público é especialmente sensível, uma vez que o Estado detém ampla capacidade de coleta, armazenamento e cruzamento de dados. Conforme observa Tasso (2020), essa assimetria exige que o tratamento de dados pelo Estado seja particularmente cuidadoso e limitado pelas finalidades públicas expressas na lei.

## **2.3 Capitalismo de Vigilância e as Novas Dimensões da Privacidade**

O conceito de capitalismo de vigilância, formulado por Zuboff, descreve um modelo econômico em que os dados comportamentais são extraídos sistematicamente para alimentar mecanismos de predição e modulação de condutas. Tal fenômeno ultrapassa o campo privado e alcança práticas governamentais, especialmente em contextos de automação decisória e vigilância estatal.

Análise recente no âmbito do Sistema Interamericano de Direitos Humanos reforça essa preocupação ao reconhecer que a privacidade deve ser compreendida como condição para o exercício de outros direitos, como liberdade de expressão, honra e identidade, exigindo do Estado políticas robustas de proteção e limitação de uso de dados (FONTANELA; FERLA; ECHER, 2022).

Essa abordagem revela que a harmonização entre LAI e LGPD não é mera questão técnica, mas elemento central para a preservação da dignidade humana em um ambiente informacional amplamente assimétrico.

### **3. A LGPD na Administração Pública**

#### **3.1 Natureza e alcance da incidência da LGPD no setor público**

A aplicação da LGPD à Administração Pública possui especificidades decorrentes da natureza jurídica do Estado e das finalidades coletivas que orientam seu funcionamento. A lei determina, em seu Art. 23, que órgãos e entidades públicas podem tratar dados pessoais sem consentimento do titular, desde que observem finalidade pública, interesse público e o exercício de competências legais.

A doutrina especializada enfatiza que o Estado, ao exercer poder de império e manejar grandes bases de dados, atua em contexto marcado por profunda assimetria informacional, o que intensifica a necessidade de controle sobre suas práticas de coleta e utilização de dados. Tasso (2020) ressalta que o tratamento estatal de dados constitui “ponto nevrálgico” das políticas públicas modernas, exigindo regulamentação rigorosa para evitar violações de direitos (TASSO, 2020).

A LGPD prevê que o setor público deve publicar as hipóteses legais de tratamento, a finalidade de cada operação e as práticas utilizadas, reforçando a *accountability* e permitindo maior controle social. Conforme mencionado por Levin (2020), o tratamento de dados pelo Estado não exclui a incidência do regime jurídico administrativo, o qual impõe deveres de legalidade, motivação e transparência (LEVIN, 2020).

A norma também distingue entidades públicas sujeitas ao regime administrativo puro (órgãos e autarquias) daquelas submetidas a regime híbrido, como empresas públicas e sociedades de economia mista, que ora se submetem às regras da iniciativa privada, ora à disciplina da Administração Direta, conforme a finalidade de sua atuação (ROSSO, 2020).

### **3.2 Princípios da LGPD aplicáveis ao setor público**

A aplicação dos princípios da LGPD no setor público constitui elemento central para a conformidade jurídica das operações estatais de tratamento de dados. A Administração, ao manejar informações pessoais em larga escala, deve observar fundamentos como finalidade, adequação, necessidade, transparência, segurança, prevenção e responsabilização, os quais funcionam como barreiras normativas à coleta excessiva ou desviante.

Esses princípios não se limitam a proclamações abstratas, mas operam como critérios concretos de contenção do poder informacional do Estado. A finalidade exige que cada operação esteja vinculada a um propósito público específico e legitimamente definido; a necessidade impõe o dever de restringir o tratamento aos dados estritamente indispensáveis à execução da atividade administrativa; e a adequação demanda compatibilidade entre os meios utilizados, as técnicas de tratamento empregadas e os objetivos declarados (TASSO, 2020).

A transparência ocupa posição estratégica nesse sistema. Ela não se confunde com a publicidade ampla e irrestrita prevista na Lei de Acesso à Informação, mas traduz um dever de explicitação clara das bases legais, das finalidades e dos fluxos informacionais, permitindo que o cidadão compreenda de que maneira seus dados são coletados, armazenados, compartilhados e descartados. Essa transparência específica da proteção de dados reforça a confiança pública, fortalece a *accountability* e possibilita o controle social.

De outro lado, os princípios de segurança e prevenção impõem a adoção de medidas técnicas e organizacionais destinadas a evitar incidentes, vazamentos e acessos não autorizados, o que se revela particularmente relevante diante da magnitude das bases de dados governamentais e do potencial impacto coletivo de falhas nesse campo.

A responsabilização, por fim, exige que os órgãos públicos demonstrem, de forma documentada, que suas operações estão em conformidade com o regime normativo de proteção de dados, o que pressupõe governança estruturada, rotinas de avaliação de risco e cultura institucional orientada ao respeito aos direitos fundamentais (LEVIN, 2020; WIMMER, 2019).

### **3.3 Bases legais específicas da Administração Pública**

No âmbito da Administração Pública, as bases legais previstas na LGPD assumem desenho próprio, em razão das funções típicas do Estado e das finalidades coletivas que justificam sua atuação. O tratamento de dados pessoais pode ser realizado, por exemplo, para o cumprimento de obrigações legais ou regulatórias, para a execução de políticas públicas, para a realização de estudos por órgãos de pesquisa, com anonimização quando possível, para a proteção da vida ou da incolumidade física de pessoas em situação de risco, bem como para o atendimento a requerimentos fundados na Lei de Acesso à Informação.

Essas hipóteses, entretanto, não significam outorga de liberdade irrestrita à Administração, mas ao contrário, estruturam e limitam o tratamento de dados, exigindo demonstração de compatibilidade entre a operação realizada, a base legal invocada e a finalidade pública subjacente (BRASIL, 2018).

A doutrina tem enfatizado que a simples invocação de uma base legal não basta para legitimar o tratamento. É necessário verificar se o uso dos dados é proporcional, se respeita o princípio da minimização e se há coerência entre a política pública em execução e as informações efetivamente coletadas e processadas.

Nesse sentido, a LGPD opera como instrumento de racionalização das práticas informacionais do Estado, deslocando a lógica de mera acumulação de dados para uma lógica de uso criterioso, justificado e controlável. Finkelstein e Finkelstein observam que, em um cenário em que a informação se tornou ativo econômico e instrumento de poder, a existência de bases legais definidas é condição mínima para impedir a formação de “zonas cinzentas” em que o tratamento de dados se dá sem transparência e sem controle democrático (FINKELSTEIN; FINKELSTEIN, 2020).

### **3.4 Deveres estruturais do Estado no tratamento de dados**

Para além dos princípios e das bases legais, a LGPD impõe ao Estado deveres estruturais que integram um modelo de governança pública de dados. A indicação de encarregado pelo tratamento de dados pessoais, por exemplo, estabelece um ponto de contato institucional entre o órgão público, a autoridade reguladora e os titulares, permitindo esclarecimentos, reclamações e orientações. A exigência de registros detalhados das operações de tratamento viabiliza a rastreabilidade, facilita auditorias internas e externas e contribui para a identificação de riscos e de práticas inadequadas.

Em operações de alto risco, sobretudo aquelas que envolvem dados sensíveis ou tecnologias sofisticadas, a elaboração de relatórios de impacto à proteção de dados mostra-se instrumento essencial para antecipar problemas, avaliar proporcionalidade e definir medidas mitigadoras.

Esses mecanismos aproximam a Administração Pública de modelos contemporâneos de governança corporativa, nos quais a responsabilidade pelo ciclo de vida da informação é compartilhada entre dirigentes, gestores e estruturas técnicas especializadas.

Nesse sentido, as pesquisas sobre governança e *compliance* de estatais sublinha que proteção de dados não deve ser vista como elemento isolado, mas como parte de um sistema mais amplo de integridade, que abrange gestão de riscos, controle interno, transparência e prestação de contas (NOHARA; GONÇALVES; ALMEIDA, 2021).

Desse modo, a LGPD contribui para redesenhar a própria arquitetura institucional do Estado, ao exigir que o tratamento de dados seja incorporado ao núcleo da gestão pública e não relegado a questões meramente tecnológicas.

#### **4 Tensões normativas entre a LAI e a LGPD**

A análise das tensões normativas entre a Lei de Acesso à Informação e a Lei Geral de Proteção de Dados evidencia que, embora os diplomas compartilhem o objetivo de fortalecer a legitimidade democrática e a proteção de direitos fundamentais, o modo como disciplinam o fluxo de informações pode gerar aparentes colisões.

A LAI, ao consagrar a publicidade como regra e o sigilo como exceção, busca assegurar controle social e transparência do Estado, dimensão amplamente reconhecida como pilar da governança pública (NOHARA; GONÇALVES; ALMEIDA, 2021).

A LGPD, por outro lado, introduz limites materiais à exposição de dados pessoais, impondo proporcionalidade, finalidade e necessidade como parâmetros para qualquer operação de tratamento. Essa colisão aparente decorre de modelos distintos de proteção de direitos: enquanto a LAI protege a cidadania por meio da informação pública, a LGPD tutela a dignidade da pessoa natural mediante a restrição do uso de dados.

Autores como Finkelstein e Finkelstein (2020) apontam que tais regimes, longe de serem incompatíveis, expressam diferentes dimensões de um mesmo esforço de contenção do poder informacional, especialmente em um contexto de crescente sensibilidade dos dados e das práticas estatais de vigilância.

Assim, torna-se imprescindível compreender como esses diplomas podem operar de forma complementar, evitando tanto a opacidade administrativa quanto a exposição indevida de indivíduos.

#### **4.1 Convergências entre transparência e proteção de dados**

Ao examinar mais detidamente os fundamentos normativos envolvidos, observa-se que LAI e LGPD apresentam convergências relevantes. Ambas se orientam por valores constitucionais como integridade, responsabilidade do Estado, limitação do poder e promoção dos direitos fundamentais. A literatura sobre governança digital enfatiza que a transparência administrativa depende, cada vez mais, da clareza sobre como dados pessoais são tratados, compartilhados e protegidos (LEVIN, 2020).

A transparência exigida pela LAI não implica divulgação indiscriminada, mas divulgação responsável, capaz de fortalecer o controle social sem violar a privacidade.

A pesquisa realizada por Fontanela, Ferla e Echer (2022) demonstra que a proteção de dados deve ser entendida como condição para o exercício pleno dos direitos informacionais em sociedades caracterizadas pelo aumento exponencial da coleta e análise de dados.

Do mesmo modo, a jurisprudência do Sistema Interamericano de Direitos Humanos reconhece que a privacidade integra o núcleo mínimo da dignidade humana e que sua violação pode comprometer outras liberdades, como expressão e participação política (CORTE IDH, 2012; 2021).

Assim, ao evitar a exposição indevida de dados, o Estado não reduz a transparência, mas qualifica-a, alinhando-se às melhores práticas internacionais e aos padrões de um governo digital ético e responsável.

#### **4.2 Conflitos aparentes e desafios interpretativos**

As tensões práticas, porém, tornam-se visíveis quando pedidos de acesso à informação envolvem dados pessoais. Nessas situações, a divulgação irrestrita pode colidir com princípios estruturantes da LGPD, como necessidade e minimização, sobretudo quando se trata de informações sensíveis ou passíveis de gerar discriminação, assim, Zuboff (2021) demonstra que, em uma sociedade marcada pela expansão do capitalismo de vigilância, a exposição de dados pode produzir efeitos duradouros sobre autonomia, identidade e liberdade individual, o que reforça a importância de limites claros ao acesso público.

Além disso, a crescente complexidade das bases estatais e a possibilidade de correlação de dados ampliam os riscos de reidentificação, mesmo quando aplicada a anonimização, como apontado por Wimmer (2019). Desafios interpretativos também decorrem de aplicações equivocadas da LGPD por parte de órgãos públicos, que, muitas vezes, negam acesso a informações com fundamento genérico na proteção de dados, sem proceder à necessária ponderação entre publicidade e privacidade, gerando opacidade indevida e fragilizando o próprio regime da LAI.

Tal comportamento confirma a advertência de Finkelstein e Finkelstein (2020) de que a proteção de dados não pode se converter em justificativa para o retrocesso democrático, mas deve atuar como instrumento de racionalização e moderação das práticas informacionais do Estado.

#### **4.3 Critérios de compatibilização normativa**

A superação desses conflitos aparentes demanda critérios claros de compatibilização normativa. A interpretação sistemática das duas leis, conforme defendem Nohara, Gonçalves e Almeida (2021), impõe que a Administração Pública reconheça transparência e proteção de dados como dimensões complementares da governança contemporânea.

Essa abordagem requer ponderação cuidadosa entre os direitos envolvidos, segundo parâmetros como adequação, necessidade e proporcionalidade, amplamente

adotados no controle de restrições a direitos fundamentais. A Corte Interamericana de Direitos Humanos reafirma reiteradamente que qualquer interferência estatal na vida privada deve ser justificada por finalidade legítima, idoneidade e proporcionalidade estrita, critério que pode orientar também a análise dos pedidos de acesso à informação (CORTE IDH, 2012; 2021).

A finalidade pública emerge, portanto, como elemento orientador central: tanto a divulgação quanto a restrição devem ser fundamentadas em objetivos legítimos do Estado, e não em razões de conveniência administrativa. Sob essa perspectiva, a compatibilização entre LAI e LGPD não depende apenas de ajustes legislativos, mas, sobretudo, de práticas administrativas fundadas em governança, integridade e responsabilidade institucional, capazes de assegurar que publicidade e privacidade coexistam sem prejuízos à democracia ou à dignidade informacional (FONTANELA; FERLA; ECHER, 2022).

## **5. Modelo integrado de governança digital**

A construção de um modelo integrado de governança digital capaz de compatibilizar as exigências de transparência da Lei de Acesso à Informação com as salvaguardas de privacidade estabelecidas pela LGPD pressupõe uma reorganização das práticas institucionais, dos fluxos informacionais e das estruturas decisórias da Administração Pública.

A governança digital não se limita à adoção de tecnologias, mas envolve a articulação entre normas, processos, responsabilidade institucional e proteção de direitos fundamentais. Nohara, Gonçalves e Almeida (2021) destacam que a governança pública contemporânea exige a integração entre integridade, transparência e gestão de riscos, de modo que o tratamento de dados pessoais deve ser compreendido como elemento estratégico para a legitimidade e a eficiência administrativa.

### **5.1 Governança orientada a risco e proteção de dados desde a concepção**

A adoção de um modelo de governança orientado por risco constitui etapa essencial na compatibilização entre LAI e LGPD. Isso implica incorporar, desde a fase de planejamento de políticas públicas e sistemas informacionais, os princípios de necessidade, minimização e proporcionalidade.



A ideia de proteção de dados desde a concepção, impõe que o Estado avalie, previamente, o impacto das operações de tratamento sobre os titulares, mitigando riscos antes que se materializem. A elaboração de Relatórios de Impacto à Proteção de Dados torna-se, assim, ferramenta indispensável, especialmente em atividades que envolvem dados sensíveis ou tecnologias preditivas.

## **5.2 Procedimentos administrativos para compatibilização prática entre LAI e LGPD**

A compatibilização entre transparência e proteção de dados depende não apenas de diretrizes normativas, mas também da implementação de procedimentos administrativos que orientem servidores e gestores públicos. Entre os elementos estruturais desse modelo, destaca-se a necessidade de fluxos decisórios claros para análise de pedidos de acesso à informação. A Administração deve, inicialmente, avaliar se o conjunto informacional solicitado envolve dados pessoais, e, em caso afirmativo, identificar se é possível realizar anonimização efetiva, substituição por dados agregados ou restrição parcial com base na ponderação entre interesse público e privacidade.

A anonimização, contudo, precisa ser tratada com rigor técnico, nessa ideia, Wimmer (2019) lembra que a simples supressão de campos identificadores não garante segurança quando há possibilidade de reidentificação por cruzamento de bases. Por essa razão, técnicas avançadas de anonimização, auditorias internas e revisões periódicas das bases de dados são essenciais para evitar que a divulgação de informações públicas se converta, inadvertidamente, em exposição de dados pessoais.

Outro elemento procedimental relevante é a documentação das decisões administrativas. A LAI exige motivação expressa para negar acesso, e a LGPD reforça a necessidade de justificar a base legal utilizada e a proporcionalidade da decisão.

Finkelstein e Finkelstein (2020) assinalam que a ausência de justificativa consistente fragiliza o controle democrático e favorece o uso inadequado da proteção de dados como argumento de ocultação de informações que deveriam ser públicas. Assim, a governança administrativa demanda transparência também nos processos decisórios internos, assegurando rastreabilidade e conformidade.

A capacitação continuada dos agentes públicos integra esse esforço. A adoção de práticas de governança digital exige formação adequada em proteção de dados,

transparência, segurança da informação e técnicas de anonimização. Nohara, Gonçalves e Almeida (2021) enfatizam que estruturas de *compliance* só funcionam quando acompanhadas de maturidade institucional, cultura organizacional comprometida com a integridade e mecanismos permanentes de avaliação.

### **5.3 Tecnologias emergentes e desafios adicionais: inteligência artificial, algoritmos e transparência automatizada**

A crescente incorporação de inteligência artificial, aprendizado de máquina e sistemas algorítmicos na gestão pública amplia exponencialmente os desafios para a compatibilização entre LAI e LGPD. Esses sistemas são capazes de processar grandes volumes de dados, identificar padrões e influenciar decisões administrativas, o que pode gerar resultados eficientes, porém potencialmente opacos. Decisões algorítmicas sem supervisão humana adequada podem reproduzir vieses, afetar desigualmente grupos vulneráveis e comprometer a igualdade de tratamento, exigindo maior rigor em transparência e governança (LEVIN, 2020).

A opacidade algorítmica também impacta a efetividade da transparência pública.

A LAI foi estruturada sob a lógica de documentos e registros administrativos tradicionais, enquanto a inteligência artificial opera sobre modelos estatísticos e bases massivas de dados cujo funcionamento nem sempre é intuitivo. Esse descompasso exige novas formas de explicabilidade, capazes de traduzir decisões automatizadas em linguagem compreensível ao cidadão.

A Corte Interamericana de Direitos Humanos, ao analisar casos envolvendo privacidade e vigilância, reforça que qualquer interferência no âmbito informacional do indivíduo deve atender aos critérios de finalidade legítima, idoneidade e proporcionalidade (CORTE IDH, 2012; 2021), parâmetros especialmente relevantes quando algoritmos influenciam políticas públicas ou decisões estatais.

A conjugação desses fatores evidencia que a compatibilização entre LAI e LGPD deve incluir também a governança algorítmica. Isso implica controles periódicos, auditorias independentes, revisão de modelos, documentação das bases utilizadas e mecanismos de supervisão humana.

Diante disso, Shoshana Zuboff (2021) adverte que sistemas preditivos alimentados por grandes fluxos de dados podem reforçar assimetrias de poder e afetar a autonomia individual, motivo pelo qual sua utilização no setor público exige salvaguardas mais robustas do que aquelas aplicadas ao setor privado.

Nesse cenário, a tecnologia não é, por si só, um problema, mas sua utilização sem mecanismos de controle pode transformar práticas administrativas legítimas em formas de vigilância incompatíveis com os direitos fundamentais. A governança digital, portanto, deve ser compreendida como conjunto integrado de políticas, processos, tecnologias e salvaguardas voltadas a assegurar que inovação e eficiência coexistam com a proteção da privacidade e com a promoção da transparência pública responsável.

## **6. Desafios regulatórios e institucionais para a compatibilização entre LAI e LGPD**

A compatibilização entre transparência pública e proteção de dados pessoais no âmbito do Estado enfrenta desafios que transcendem a interpretação jurídica das normas e alcançam dimensões estruturais, culturais, tecnológicas e organizacionais da Administração Pública. Embora a LAI e a LGPD componham um único sistema de proteção de direitos fundamentais, sua aplicação integrada depende da existência de arranjos institucionais capazes de sustentar práticas administrativas coerentes, de assegurar segurança jurídica e de promover governança digital orientada por valores democráticos.

Um dos primeiros desafios reside na fragmentação normativa e na ausência de diretrizes mais detalhadas sobre como proceder à ponderação entre publicidade e privacidade. A LGPD estabelece princípios e bases legais, mas não fornece parâmetros objetivos para a tomada de decisão em casos concretos que envolvam colisões com o direito de acesso à informação.

Da mesma forma, a LAI prevê hipóteses de sigilo e proteção de informações pessoais, porém sem oferecer critérios metodológicos para sua harmonização com o regime de proteção de dados. Essa lacuna normativa gera interpretações divergentes entre órgãos públicos, resultando em práticas inconsistentes e, muitas vezes, incompatíveis com uma governança digital responsável. Como apontam Nohara, Gonçalves e Almeida (2021), a ausência de uniformidade interpretativa compromete a integridade institucional e fragiliza a confiabilidade dos mecanismos de transparência.

Outro obstáculo relevante diz respeito à capacidade técnica e operacional da Administração Pública. A aplicação adequada da LGPD requer conhecimentos especializados em segurança da informação, técnicas de anonimização, arquitetura de sistemas, governança de dados e auditoria algorítmica.

Entretanto, estudos sobre transformação digital na esfera estatal revelam que muitos órgãos ainda operam com infraestruturas tecnológicas defasadas, recursos humanos insuficientes e estruturas organizacionais pouco preparadas para lidar com o volume e a sensibilidade dos dados sob sua custódia (LEVIN, 2020). Essa ausência de maturidade institucional dificulta tanto a implementação das salvaguardas de proteção de dados quanto o atendimento eficiente às exigências de transparência da LAI.

Os riscos relacionados à vigilância estatal e ao uso ampliado de tecnologias de monitoramento também representam desafio central. O fenômeno descrito por Zuboff (2021) como “capitalismo de vigilância” evidencia que a coleta massiva e o tratamento contínuo de dados podem reforçar assimetrias informacionais e ampliar o poder de controle sobre indivíduos, sobretudo quando associadas a tecnologias preditivas e algoritmos opacos.

Nessa análise, Fontanela, Ferla e Echer (2022) observam que, em contextos dessa natureza, a falta de limites adequados ao tratamento de dados pode resultar em cenários de vigilância incompatíveis com a proteção da privacidade e da autodeterminação informativa. Assim, a utilização de tecnologias emergentes pela Administração, como inteligência artificial e análise comportamental, deve ser acompanhada de mecanismos de governança algorítmica, com ênfase em supervisão humana, explicabilidade e prevenção de vieses.

Do ponto de vista institucional, a coordenação entre órgãos responsáveis por transparência, tecnologia e proteção de dados configura desafio adicional. No Brasil, a Controladoria-Geral da União (CGU), a Autoridade Nacional de Proteção de Dados (ANPD), os órgãos de controle interno e externo, e as unidades de tecnologia da informação possuem competências parcialmente sobrepostas no que tange à governança da informação. A ausência de articulação sistemática entre essas instâncias pode produzir orientações contraditórias, dificultando a adoção de práticas uniformes pelos órgãos públicos. Finkelstein e Finkelstein (2020) reforçam que a governança de dados demanda

atuação coordenada e visão sistêmica, sob pena de se transformar em um mosaico de iniciativas isoladas, sem impacto efetivo na proteção de direitos.

Outro desafio significativo relaciona-se à cultura organizacional da Administração Pública. A transição de um modelo burocrático tradicional para um modelo orientado por dados exige não apenas mudanças tecnológicas, mas reformulação de mentalidades, hábitos institucionais e incentivos internos.

Muitas unidades administrativas ainda compreendem a proteção de dados como entrave ao funcionamento institucional, ou interpretam a LGPD como justificativa para a ampliação indevida do sigilo. Essa visão distorcida compromete a efetividade da transparência e reforça posturas defensivas, contrárias ao espírito republicano da LAI.

Assim, para superar essa resistência, é necessária uma política contínua de formação e capacitação, aliada a mecanismos de responsabilização e incentivos à conformidade (NOHARA; GONÇALVES; ALMEIDA, 2021).

A falta de investimentos em tecnologia e segurança da informação constitui elemento adicional de vulnerabilidade. Sistemas desatualizados, ausência de criptografia, fragilidade no controle de acessos e inexistência de rotinas de auditoria aumentam o risco de incidentes, comprometendo não apenas a proteção de dados pessoais, mas também a credibilidade das instituições públicas.

Já Wimmer (2019) destaca que vulnerabilidades dessa natureza têm impacto ampliado no setor público, pois incidentes envolvendo dados governamentais afetam, simultaneamente, milhões de cidadãos e comprometem a confiança coletiva no Estado. Assim, a consolidação de uma arquitetura tecnológica segura é pré-requisito para que a Administração possa divulgar informações públicas de forma responsável, sem risco de exposição indevida.

Por fim, a ausência de mecanismos eficazes de fiscalização e responsabilização dificulta a consolidação de um ambiente regulatório maduro. A LGPD prevê sanções e orientações aplicáveis ao setor público, mas sua efetividade depende da capacidade institucional da ANPD, ainda em processo de estruturação. Do mesmo modo, a atuação dos órgãos de controle deve evoluir para incorporar critérios de governança de dados em suas auditorias, avaliando não apenas a regularidade documental, mas a efetividade das práticas informacionais.

A Corte Interamericana de Direitos Humanos tem reiterado que a proteção da privacidade exige ações positivas dos Estados, sob pena de vulneração de direitos essenciais e enfraquecimento da democracia (CORTE IDH, 2012; 2021). Tal diretriz reforça a necessidade de mecanismos de responsabilização que impeçam a negligência e estimulem a adoção de padrões elevados de governança.

A superação desses desafios requer transformação institucional abrangente, baseada em visão sistêmica da governança digital e na incorporação simultânea dos valores da transparência e da proteção de dados. Trata-se de processo contínuo, dependente de maturidade administrativa, investimento estatal, supervisão regulatória e participação social. Somente por meio desse conjunto articulado de esforços será possível assegurar que a LAI e a LGPD operem de forma complementar, fortalecendo a democracia, a integridade pública e a dignidade informacional dos cidadãos.

## **CONCLUSÃO**

A análise empreendida ao longo desta pesquisa demonstra que a governança digital contemporânea exige a harmonização entre dois pilares normativos fundamentais: a transparência administrativa, consagrada pela Lei de Acesso à Informação, e a proteção de dados pessoais, assegurada pela Lei Geral de Proteção de Dados. Embora ambos os diplomas se orientem por valores constitucionais convergentes, como controle democrático, limitação do poder estatal e tutela da dignidade humana, sua operacionalização prática revela tensões que precisam ser resolvidas por meio de mecanismos interpretativos, procedimentais e institucionais adequados.

A investigação evidenciou que a LGPD introduz um regime jurídico que reordena profundamente a forma como o Estado trata dados pessoais, impondo princípios de finalidade, necessidade, transparência, segurança e responsabilidade que não apenas qualificam a atuação administrativa, mas também atuam como contrapesos ao potencial de vigilância do poder público. Tais salvaguardas tornam-se particularmente relevantes em um contexto marcado pelo fenômeno identificado por Zuboff (2021) como capitalismo de vigilância, no qual o acúmulo massivo de dados e o uso de tecnologias preditivas criam riscos inéditos à autonomia e à identidade informacional dos indivíduos.

Levando em consideração as pesquisas realizadas observa-se que a proteção de dados não constitui obstáculo à transparência coletiva, mas parte essencial de um

ordenamento jurídico que busca equilibrar publicidade e privacidade com vistas à preservação da democracia.

Ao mesmo tempo, a LAI mantém sua centralidade como instrumento de controle social e de fortalecimento da integridade pública. Como salientam Nohara, Gonçalves e Almeida (2021), a transparência permanece elemento estruturante da governança estatal, e sua efetividade depende da clareza, acessibilidade e qualidade das informações disponibilizadas ao público. A compatibilização entre LAI e LGPD, portanto, não implica redução da publicidade, mas transformação das práticas administrativas, de modo que a divulgação seja feita com responsabilidade, observando-se limites proporcionais e técnicas adequadas de anonimização, quando necessário.

A proposta de modelo integrado de governança digital apresentada, demonstra que a solução para esses desafios não se encontra na prevalência automática de uma norma sobre a outra, mas na construção de fluxos decisórios, práticas administrativas, políticas internas e mecanismos tecnológicos que permitam ao Estado decidir, caso a caso, a forma mais adequada de compatibilização. A adoção de governança orientada a risco, proteção de dados desde a concepção, documentação das decisões e auditorias constantes revela-se fundamental para assegurar que a Administração Pública utilize informações de forma estratégica e responsável, preservando tanto o interesse público quanto os direitos individuais.

Os desafios mapeados, reforçam que a efetividade desse modelo depende de fatores estruturais, como capacidade técnica, investimentos em segurança da informação, ações coordenadas entre diferentes órgãos públicos e desenvolvimento de uma cultura institucional voltada à integridade e à proteção de dados. A evolução tecnológica acelerada, especialmente com o uso de inteligência artificial e sistemas algorítmicos, amplia a necessidade de governança robusta e de supervisão humana, conforme apontam estudos nacionais e internacionais.

A jurisprudência da Corte Interamericana de Direitos Humanos, ao enfatizar a importância da proporcionalidade e da finalidade legítima nas interferências estatais sobre a privacidade, oferece diretrizes relevantes para o cenário brasileiro, indicando que transparência e proteção de dados devem caminhar juntas como garantias recíprocas da dignidade humana (CORTE IDH, 2012; 2021).

Diante desse panorama, conclui-se que a compatibilização entre LAI e LGPD não constitui um conflito insolúvel, mas uma tarefa hermenêutica e institucional que exige maturidade regulatória e compromisso democrático. A convergência entre esses diplomas fortalece o Estado de Direito ao impedir tanto o sigilo indevido quanto a exposição excessiva, preservando a autonomia informacional dos cidadãos e assegurando que a informação pública cumpra seu papel social. A consolidação de práticas de governança digital responsáveis representa, assim, o caminho para uma Administração Pública capaz de inovar, proteger direitos e manter-se transparente, íntegra e alinhada às exigências de uma sociedade orientada por dados.

As lacunas de pesquisa devem aprofundar questões relativas à governança algorítmica, aos limites do uso estatal de inteligência artificial, às técnicas avançadas de anonimização e à efetividade dos mecanismos de auditoria pública. Em um cenário de rápida evolução tecnológica, tais temas tornam-se indispensáveis para garantir que a proteção de dados e a transparência pública não apenas coexistam, mas se reforcem mutuamente como fundamentos de uma sociedade democrática informacionalmente justa.

## **REFERÊNCIAS**

ALMEIDA, Renato José de; NOHARA, Irene Patrícia; GONÇALVES, Lucas Sérgio. Governança e Compliance das Estatais. São Paulo: Thomson Reuters Brasil, 2021.

BRASIL. Constituição da República Federativa do Brasil de 1988.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Lei de Acesso à Informação. Diário Oficial da União, Brasília, 18 nov. 2011.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, 15 ago. 2018.

CORTE INTERAMERICANA DE DIREITOS HUMANOS. Relatório Anual da Corte Interamericana de Direitos Humanos 2012. San José, Costa Rica, 2012.

CORTE INTERAMERICANA DE DIREITOS HUMANOS. Relatório Anual da Corte Interamericana de Direitos Humanos 2021. San José, Costa Rica, 2021.

FINKELSTEIN, Cláudia; FINKELSTEIN, Bruno. A LGPD no setor público: desafios, limites e possibilidades. In: MORAES, Pablo (org.). A LGPD e o Poder Público. São Paulo: Editora Revista dos Tribunais, 2021. p. 269–289.



FONTANELA, Diego; FERLA, Marcela; ECHER, Isadora. Capitalismo de Vigilância e a Proteção da Privacidade no Sistema Interamericano de Direitos Humanos. In: Anais do CONPEDI. Belo Horizonte: CONPEDI, 2022. p. 119–140.

LEVIN, Anna. Fundamentos jurídicos da proteção de dados no setor público. In: MORAES, Pablo (org.). A LGPD e o Poder Público. São Paulo: Editora Revista dos Tribunais, 2021. p. 243–268.

MORAES, Pablo (org.). A LGPD e o Poder Público. São Paulo: Editora Revista dos Tribunais, 2021.

PEREIRA, Ana Virgínia; PAIVA, Luiz Gustavo. Organização Administrativa e Inteligência Artificial na Administração Pública. Belo Horizonte: Universidade Federal de Minas Gerais, 2023.

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

TASSO, Felipe. O tratamento de dados pessoais pelo Poder Público: limites e possibilidades. In: MORAES, Pablo (org.). A LGPD e o Poder Público. São Paulo: Editora Revista dos Tribunais, 2021. p. 243–268.

WIMMER, Miriam. Proteção de dados pessoais e políticas públicas. In: MORAES, Pablo (org.). A LGPD e o Poder Público. São Paulo: Editora Revista dos Tribunais, 2021. p. 121–144.

ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder. Tradução: George Schlesinger. Rio de Janeiro: Intrínseca, 2021.