RJNM
ISSN 2675-4312

Received: 13/10/2026 - **Accepted:** 11/11/2026
Vol: 07.11
DOI: 10.66104/29137t27
Pages: 1-18

PROTEÇÃO DA IDENTIDADE DIGITAL: LIMITES JURIDICOS ENTRE A PRIVACIDADE E A TRANSPARÊNCIA PÚBLICA.

PROTECTION OF DIGITAL IDENTITY: LEGAL BOUNDARIES BETWEEN PRIVACY AND PUBLIC TRANSPAREN

PROTECCIÓN DE LA IDENTIDAD DIGITAL: LÍMITES JURÍDICOS ENTRE LA PRIVACIDAD Y LA TRANSPARENCIA PÚBLICA.

Camilly Rocha Fialho Ribeiro
Graduanda em Direito, Faculdade de Ensino Superior de Linhares
Endereço: Linhares, Espírito Santo, Brasil
E-mail: camillyrochafialho@gmail.com

Jakeline Martins Silva Rocha

Graduada em Direito pela UFMA- Universidade Federal do Maranhão. Especialista em Direito Empresarial pela FVC - Faculdade Vale do Cricaré. Especialista em Educação e Supervisão pela FVC. Mestra em Gestão Social, Educação e Desenvolvimento Regional pela FVC. Advogada. No Centro Universitário Vale do Cricaré é professora da Graduação em Direito e Coordenadora e orientadora do NPJ/UNIVC. Na FACELI - Faculdade de Ensino Superior de Linhares/ES/ bloco de Direito Privado. É Membro da CPA - Comissão Permanente de Avaliação/ Faceli. Membro titular do CONSUP - Conselho Superior/Faceli e membro suplente do CONCUR-Conselho Curador da Fundação Faceli. É professora do grupo "Temas Avançados de Direito Privado". Conselheira da 12 Subseção, OAB/ES (2022-2024). Vice-diretora administrativa da ESA (norte do ES)- Escola Superior da Advocacia/ES (2019 a 2021). Secretária-Geral Adjunta da 12 Subseção/OAB-ES. (2025-2027). Procuradora-Geral da Fundação Faceli (2024-atual). E-mail:jakeline.rocha@faceli.edu e jakeline.rocha@ivc.br

Resumo

O presente artigo analisa os limites jurídicos entre a proteção da identidade digital e a transparência pública no ordenamento jurídico brasileiro. A partir da elevação da proteção de dados pessoais à condição de direito fundamental pela Emenda Constitucional nº 115/2022, examina-se sua relação com o direito de acesso à informação e com o princípio da publicidade administrativa. A pesquisa possui

CC BY

RJNM
ISSN 2675-4312

Received: 13/10/2026 - **Accepted:** 11/11/2026
Vol: 07.11
DOI: 10.66104/29137t27
Pages: 1-18

natureza qualitativa, caráter exploratório e abordagem predominantemente jurídico-dogmática, desenvolvida mediante pesquisa bibliográfica e documental, com análise da Constituição Federal, da Lei de Acesso à Informação, da Lei Geral de Proteção de Dados Pessoais, do Marco Civil da Internet e de precedentes judiciais relacionados ao tema. Investiga-se, especialmente, em que medida a proteção de dados pessoais pode limitar a divulgação de informações pelo Poder Público e quais critérios permitem compatibilizar privacidade, proteção de dados e controle social. Sustenta-se que a relação entre a Lei Geral de Proteção de Dados Pessoais (LGPD) e a Lei de Acesso à Informação (LAI) não deve ser compreendida como oposição absoluta entre proteção de dados e transparência, mas como uma relação de compatibilização normativa, na qual a divulgação de informações pessoais deve observar finalidade, necessidade, adequação, fundamento jurídico e proporcionalidade. Conclui-se que a proteção de dados pessoais não constitui, por si só, fundamento suficiente para afastar o dever de transparência, assim como a publicidade administrativa não autoriza a divulgação indiscriminada de informações pessoais.

Palavras-chave: identidade digital, proteção de dados pessoais, transparência pública, lei de acesso à informação e privacidade.

Abstract

This article analyzes the legal boundaries between the protection of digital identity and public transparency within the Brazilian legal system. Following the elevation of personal data protection to the status of a fundamental right via Constitutional Amendment No. 115/2022, the study examines its relationship with the right of access to information and the principle of administrative publicity. The research is qualitative and exploratory in nature, employing a predominantly legal-dogmatic approach. It is based on a review of literature and legal documents, including an analysis of the Federal Constitution, the Access to Information Law, the General Personal Data Protection Law (LGPD), the Brazilian Civil Rights Framework for the Internet (Marco Civil da Internet), and relevant judicial precedents. Specifically, the study investigates the extent to which personal data protection may limit

CC BY

RJNM
ISSN 2675-4312

Received: 13/10/2026 - **Accepted:** 11/11/2026
Vol: 07.11
DOI: 10.66104/29137t27
Pages: 1-18

the disclosure of information by public authorities, as well as the criteria that allow for the reconciliation of privacy, data protection, and social oversight. It is argued that the relationship between the General Personal Data Protection Law (LGPD) and the Access to Information Law (LAI) should not be viewed as an absolute opposition between data protection and transparency, but rather as a matter of normative reconciliation—where the disclosure of personal information must adhere to principles of purpose, necessity, adequacy, legal basis, and proportionality. The article concludes that the protection of personal data does not, in itself, constitute sufficient grounds to set aside the duty of transparency; conversely, the principle of administrative publicity does not authorize the indiscriminate disclosure of personal information.

Keywords: digital identity, personal data protection, public transparency, access to information law, and privacy.

Resumen

El presente artículo analiza los límites jurídicos entre la protección de la identidad digital y la transparencia pública en el ordenamiento jurídico brasileño. A partir de la elevación de la protección de datos personales a la categoría de derecho fundamental mediante la Enmienda Constitucional n.º 115/2022, se examina su relación con el derecho de acceso a la información y con el principio de publicidad administrativa. La investigación es de naturaleza cualitativa, carácter exploratorio y enfoque predominantemente jurídico-dogmático; se desarrolló mediante una investigación bibliográfica y documental que incluye el análisis de la Constitución Federal, la Ley de Acceso a la Información, la Ley General de Protección de Datos Personales, el Marco Civil de Internet y precedentes judiciales relacionados con el tema. Se indaga, en particular, en qué medida la protección de datos personales puede limitar la divulgación de información por parte del Poder Público y qué criterios permiten compatibilizar la privacidad, la protección de datos y el control social. Se sostiene que la relación entre la Ley General de Protección de Datos Personales (LGPD) y la Ley de Acceso a la Información (LAI) no debe entenderse como una oposición absoluta entre la protección de datos y la transparencia, sino como una relación de compatibilización normativa, en la cual la divulgación de información personal debe observar los principios de finalidad, necesidad, adecuación, fundamento jurídico y proporcionalidad. Se concluye que la protección de datos personales no constituye, por sí sola, un fundamento suficiente para eximir del deber de transparencia; del mismo modo, la publicidad administrativa no autoriza la divulgación indiscriminada de información personal.

Palabras clave: identidad digital, protección de datos personales, transparencia pública, ley de

CC BY

RJNM
ISSN 2675-4312

Received: 13/10/2026 - **Accepted:** 11/11/2026
Vol: 07.11
DOI: 10.66104/29137t27
Pages: 1-18

acceso a la información y privacidad.

1. Introdução

Na era informacional, o indivíduo desgarrou-se de seus contornos físicos para transmutar-se em um fluxo ininterrupto de dados rastreáveis e mercantilizáveis, fazendo com que o corpo humano deixasse de ser a fronteira final da identidade. Essa metamorfose alterou a própria espinha dorsal das relações jurídicas, forçando o Direito a repensar seus institutos clássicos para proteger a pessoa humana de ser objetificada pela sociedade em rede. É nesse contexto de transição que a doutrina aponta a insuficiência dos modelos tradicionais de proteção, como nos mostra Doneda (2020, p. 94):

> A tutela remedial, típica do direito subjetivo, não é mais do que um instrumento entre outros que podem ser utilizados para a tutela da privacidade, e de forma alguma é a estrutura na qual deva necessariamente se concretizar. A ela faltam os instrumentos adequados à realização da função promocional da tutela da privacidade como meio de proteção da pessoa humana e da atuação da cláusula geral da proteção da personalidade; nela igualmente não é concebida a dimensão coletiva na qual se insere a problemática da privacidade.

Nesse cenário, a identidade digital converte-se em extensão indissociável da personalidade do ser humano, demandando uma tutela jurídica compatível com sua nova relevância. Diante dessa transformação, o Direito Constitucional é convocado a reafirmar a sua vocação histórica, na qual a Constituição assume a missão de organizar racionalmente a sociedade, configurando-se como “o estatuto do poder e o instrumento jurídico com que a sociedade se premune contra a tendência imemorial de abuso dos governantes” (Mendes; Branco, 2012, p. 57).

No ordenamento jurídico brasileiro, a proteção dessa dimensão existencial ganhou contornos definitivos com a promulgação da Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Ao inserir a proteção de dados pessoais no rol dos

CC BY

RJNM
ISSN 2675-4312

Received: 13/10/2026 - **Accepted:** 11/11/2026
Vol: 07.11
DOI: 10.66104/29137t27
Pages: 1-18

direitos e garantias fundamentais (artigo 5º, inciso LXXIX, da Constituição Federal), o legislador reconheceu a autodeterminação informativa como elemento essencial da dignidade humana na sociedade digital, exigindo que qualquer tratamento de dados observe estritamente os princípios da finalidade, necessidade e transparência. Paralelamente, a legislação infraconstitucional evoluiu para dar materialidade a essa garantia, na qual o Marco Civil da Internet (Lei nº 12.965/2014) estabeleceu os primeiros princípios gerais de proteção da privacidade no ambiente digital, mas foi com a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) que o país consolidou um regime jurídico orgânico e abrangente, aplicável tanto ao setor privado quanto ao setor público.

Contudo, a consolidação desse arcabouço protetivo suscita importantes tensionamentos com outro pilar do Estado Democrático de Direito: a transparência pública. A Lei de Acesso à Informação (LAI – Lei nº 12.527/2011) consagra a publicidade como regra e o sigilo como exceção na Administração Pública, garantindo aos cidadãos o direito de fiscalizar atos governamentais e exigir accountability. Observa-se, na prática, uma crescente utilização da LGPD como justificativa para negar acesso a informações públicas, configurando distorção de sua finalidade e comprometendo o controle social democrático. Surge, portanto, um questionamento central: como compatibilizar a proteção da identidade digital com a necessidade de transparência dos atos públicos?

O presente artigo tem por objetivo investigar os limites jurídicos entre a privacidade e a transparência pública, analisando a tensão normativa entre LGPD e LAI. Pretende-se demonstrar que, mediante interpretação sistemática e aplicação dos princípios da proporcionalidade e razoabilidade na colisão de direitos fundamentais, é possível harmonizar a tutela da identidade digital e a transparência democrática, assegurando a proteção do cidadão sem retrocessos no dever estatal de prestar contas.

A pesquisa desenvolvida neste artigo possui natureza qualitativa, caráter exploratório e abordagem predominantemente jurídico-dogmática. Quanto aos

CC BY

RJNM
ISSN 2675-4312

Received: 13/10/2026 - **Accepted:** 11/11/2026
Vol: 07.11
DOI: 10.66104/29137t27
Pages: 1-18

procedimentos técnicos, foi realizada pesquisa bibliográfica e documental, com exame de legislação, atos normativos, documentos institucionais, produção doutrinária e decisões judiciais relacionadas à proteção de dados pessoais, à privacidade e ao acesso à informação no âmbito da Administração Pública.

A análise bibliográfica concentrou-se em obras de referência sobre proteção de dados pessoais, privacidade, direitos fundamentais, poder informacional e sociedade em rede, com destaque para os trabalhos de Doneda, Bioni, Alexy e Foucault. A pesquisa documental compreendeu, especialmente, a Constituição Federal, a Lei nº 12.527/2011 (Lei de Acesso à Informação), a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), o Marco Civil da Internet e documentos orientativos produzidos pela Autoridade Nacional de Proteção de Dados (ANPD) e por órgãos públicos responsáveis pela implementação das políticas de transparência e acesso à informação.

No campo jurisprudencial, foram examinados precedentes do Supremo Tribunal Federal e do Superior Tribunal de Justiça relacionados à publicidade de informações funcionais de agentes públicos, ao tratamento de dados pessoais pelo Poder Público e às consequências jurídicas decorrentes da exposição ou disponibilização indevida de dados pessoais. A seleção dos precedentes considerou sua pertinência direta com o problema de pesquisa e sua relevância para a compreensão da relação entre proteção de dados e transparência administrativa.

A análise adotou perspectiva sistemática, buscando identificar os pontos de convergência e de tensão entre os regimes jurídicos de proteção de dados pessoais e de acesso à informação. Não se pretendeu realizar levantamento estatístico da jurisprudência brasileira, mas examinar, de forma qualitativa, os fundamentos normativos e argumentativos empregados na solução dos conflitos entre privacidade, proteção de dados e publicidade administrativa.

3 A IDENTIDADE DIGITAL E A ASSIMETRIA DE PODER

CC BY

RJNM
ISSN 2675-4312

Received: 13/10/2026 - **Accepted:** 11/11/2026
Vol: 07.11
DOI: 10.66104/29137t27
Pages: 1-18

A identidade digital representa o conjunto de informações, atributos e características que individualizam e identificam uma pessoa no ambiente virtual. Diferentemente da identidade física tradicional, a identidade digital constrói-se a partir de dados pessoais dispersos em múltiplas plataformas, integrando os direitos da personalidade como desdobramento contemporâneo dos direitos à intimidade e à vida privada. A doutrina civilista contemporânea reconhece que a identidade digital não constitui mera extensão analógica da identidade física, mas sim nova dimensão da personalidade humana que demanda proteção jurídica específica. A inserção desses dados em um ambiente de alto processamento informacional redimensionou o valor da identidade, transformando os dados pessoais na força motriz do mercado. Bioni (2019) esclarece a gravidade dessa mercantilização da identidade e a transição para o que denomina "economia de vigilância":

> A informação deve ser, assim, convertida em um conhecimento, a fim de torná-la produtiva e estratégica para a atividade empresarial. Por isso, é a matéria-prima de uma economia redimensionada pelos avanços das TICs, destacando-se os dados pessoais dos cidadãos que passam a ditar uma (nova) lógica de acumulação de capital para a geração de riquezas. (Bioni, 2019, p. 38-39).

Nesta conjuntura, instaura-se uma profunda assimetria de poder entre o titular dos dados e os agentes que controlam o fluxo informacional. A estratégia normativa baseada exclusivamente no "consentimento" do indivíduo, forjada em décadas passadas, revela-se insuficiente diante das limitações cognitivas e da hipervulnerabilidade do cidadão moderno. Bioni (2019, p. 188) critica essa delegação irreal de responsabilidade na autoproteção de dados, entendendo que se trata, sobretudo, de um "processo de revigoramento dessa estratégia regulatória que, forjada nos anos 1980, conduz a um refratário protagonismo do consentimento". Para o autor, o saldo desse percurso é "apostar no indivíduo como um ser capaz, racional

CC BY

RJNM
ISSN 2675-4312

Received: 13/10/2026 - **Accepted:** 11/11/2026
Vol: 07.11
DOI: 10.66104/29137t27
Pages: 1-18

e hábil para controlar as suas informações pessoais. Tem-se, assim, um quadro regulatório encapsulado por uma compreensão reducionista do conteúdo a que se deve referir autodeterminação informacional".

Ademais, a proteção de dados pessoais como direito autônomo da personalidade rompe com a estrita dicotomia histórica entre o que é público e o que é privado. Bioni (2019) demonstra que mesmo dados manifestamente públicos, quando agregados e submetidos a processos de decisões automatizadas, podem gerar a formação de perfis comportamentais, a chamada *profiling*, que estigmatizam o cidadão e afetam o livre desenvolvimento da sua personalidade. Esta assimetria adquire contornos ainda mais críticos quando o controlador dos dados é o próprio Estado, situação em que a entrega de informações é frequentemente compulsória para o acesso a políticas públicas e o exercício da cidadania. A proteção de dados assume, assim, o papel de direito da personalidade autônomo, não apenas como regra de mercado, mas como limite democrático fundamental para proteger o livre desenvolvimento da pessoa humana contra os abusos do poder informacional estatal.

4 O CONFLITO APARENTE: PRIVACIDADE VERSUS TRANSPARÊNCIA

O direito fundamental à proteção de dados e à autodeterminação informativa encontra-se, frequentemente, em aparente oposição com o princípio da publicidade administrativa e o direito de acesso à informação, regido pela Lei nº 12.527/2011 (LAI). A transparência pública é pilar do Estado Democrático de Direito, justificando-se sob perspectivas republicanas para permitir o controle social, inibir práticas ilícitas e possibilitar a responsabilização de agentes públicos. Todavia, observa-se na prática da Administração Pública a crescente utilização da Lei Geral de Proteção de Dados Pessoais (LGPD) como justificativa para negar pedidos de acesso à informação formulados com base na LAI, sob o argumento genérico da proteção da privacidade.

CC BY

RJNM
ISSN 2675-4312

Received: 13/10/2026 - **Accepted:** 11/11/2026
Vol: 07.11
DOI: 10.66104/29137t27
Pages: 1-18

A doutrina e a jurisprudência brasileiras vêm enfrentando essa tensão normativa que pode ser solucionada por meio de interpretação sistemática. A proteção de dados não pode servir de subterfúgio para a opacidade estatal: o segredo deve ser exceção, e a transparência, regra, desde que qualificada. A divulgação de dados pessoais exige base legal específica e interesse público predominante que justifique a restrição à privacidade. Essa harmonização pressupõe compreender que a LGPD não se limita à tutela do segredo. Como observa Bioni (2019, p. 127-128), a proteção de dados rompe com a distinção rígida entre público e privado:

> A dinâmica de proteção dos dados pessoais foge à dicotomia do público e do privado, diferenciando-se substancialmente do direito à privacidade. [...] Propugnar que o direito à proteção dos dados pessoais seria uma mera evolução do direito à privacidade é uma construção dogmática falha que dificulta a sua compreensão. É um direito que opera fora da lógica binária do público e do privado, bastando que a informação esteja atrelada a uma pessoa – conceito de dado pessoal – para deflagrá-lo.

A materialização dessa distorção normativa pode ser identificada na prática administrativa recente do Estado brasileiro. Um levantamento realizado pela agência especializada em acesso a informações públicas Fiquem Sabendo[1] revelou, em 2021, que a Controladoria-Geral da União (CGU) e a Comissão Mista de Reavaliação de Informações (CMRI) analisaram dezenas de pedidos de acesso à informação indevidamente negados por órgãos federais sob a justificativa de aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD). Entre os casos analisados, destacam-se a recusa do Ministério da Agricultura da época em fornecer dados

[1] Levantamento disponível em: https://fiquemsabendo.com.br/transparencia/lgpd-negativa-cgu/. Acesso em: 29 set. 2026.

CC BY

RJNM
ISSN 2675-4312

Received: 13/10/2026 - **Accepted:** 11/11/2026
Vol: 07.11
DOI: 10.66104/29137t27
Pages: 1-18

relativos a proprietários rurais autuados por desmatamento e as sucessivas negativas do Gabinete de Segurança Institucional (GSI) em disponibilizar registros de visitantes do Palácio do Planalto.

Ao enquadrar o trânsito de pessoas em instalações do Poder Executivo como hipótese de proteção de dados pessoais, a Administração Pública acaba por conferir à garantia da privacidade uma extensão incompatível com as exigências de transparência e controle social que regem a atividade estatal. Nesses episódios, a CGU interveio para reafirmar a prevalência da Lei de Acesso à Informação (LAI), consolidando o entendimento de que registros de entrada e saída de edifícios públicos podem apresentar relevância para a identificação de potenciais conflitos de interesse e, por conseguinte, submeter-se a regime de publicidade orientado pelo interesse público preponderante.

Portanto, mesmo que um dado seja de interesse público e deva ser divulgado por força da LAI, ele continua sendo um dado pessoal protegido pela LGPD, o que exige que o seu tratamento pelo Estado ocorra de forma ética, segura e proporcional. Para solucionar essa tensão normativa nos casos concretos, o ordenamento jurídico exige a aplicação criteriosa do princípio da proporcionalidade na colisão de direitos fundamentais. Conforme assentado pela doutrina clássica de Robert Alexy (2008), a proporcionalidade desdobra-se na verificação da adequação (a medida deve ser apta a alcançar o objetivo almejado), necessidade (a medida deve ser a menos restritiva possível dentre as alternativas disponíveis) e proporcionalidade em sentido estrito (os benefícios da medida devem superar seus custos).

O “interesse público preponderante” constitui o critério hermenêutico central nessa ponderação. No julgamento do ARE nº 639.228 (Tema 483 de Repercussão Geral), o Supremo Tribunal Federal (STF) assentou a tese de que é legítima a publicação do nome e da remuneração de servidores públicos em portais de transparência. A *ratio decidendi* da Suprema Corte fundamentou-se na premissa de que o agente público, ao atuar em nome do Estado e ser remunerado pelo erário, submete-se a um regime diferenciado de publicidade, sofrendo uma redução legítima

CC BY

RJNM
ISSN 2675-4312

Received: 13/10/2026 - **Accepted:** 11/11/2026
Vol: 07.11
DOI: 10.66104/29137t27
Pages: 1-18

e proporcional da sua expectativa de privacidade em prol do princípio republicano da prestação de contas. Contudo, a Corte ressalvou que informações relativas à esfera estritamente íntima (como dados médicos, convicções ou endereço residencial) permanecem intangíveis, por não guardarem nexo causal com o exercício da função pública.

Noutra vertente, quando o Estado atua como controlador massivo de dados de particulares, o STF impôs freios rigorosos. No julgamento conjunto das ADIs nº 6.387, 6.388, 6.389 e 6.390/DF, a Corte suspendeu a eficácia da Medida Provisória nº 954/2020, que obrigava as empresas de telecomunicações a partilhar dados de milhões de utilizadores com o IBGE (Instituto Brasileiro de Geografia e Estatística). O Tribunal não apenas consolidou, de forma pioneira, o reconhecimento da proteção de dados como um direito fundamental autônomo, como estabeleceu que o tratamento de dados pelo Poder Público não confere ao Estado um "cheque em branco". A decisão sublinhou que a requisição de dados exige finalidade específica, estrita necessidade e, sobretudo, a demonstração de salvaguardas técnicas de segurança que impeçam o desvio de finalidade, elementos ausentes na referida norma.

No âmbito do Superior Tribunal de Justiça (STJ), a jurisprudência tem avançado na fixação das consequências jurídicas perante as falhas na governança e tutela destas informações. Ao julgar o REsp nº 1.758.761/SP, a Corte Superior passou a delinear o rigoroso escopo da responsabilidade civil por vazamento de dados, assinalando que a exposição indevida de dados pessoais, especialmente os sensíveis, pode configurar dano moral presumido *(in re ipsa).* Este entendimento eleva substancialmente o ónus de cautela do Estado e dos entes controladores, evidenciando que a proteção da identidade digital não é uma mera formalidade administrativa, mas um bem jurídico cuja violação atrai responsabilização imediata e severa.

CC BY

RJNM
ISSN 2675-4312

Received: 13/10/2026 - **Accepted:** 11/11/2026
Vol: 07.11
DOI: 10.66104/29137t27
Pages: 1-18

5 O PANÓPTICO DIGITAL E O PRINCÍPIO DA NÃO DISCRIMINAÇÃO ALGORÍTMICA

O tratamento de dados pessoais pelo Poder Público (capítulo IV da LGPD) possui especificidades notáveis, uma vez que a Administração baseia-se primordialmente na execução de políticas públicas e no cumprimento de obrigações legais, não dependendo exclusivamente do consentimento do titular. Esta prerrogativa confere ao Estado uma responsabilidade redobrada na gestão destes ativos informacionais, exigindo a implementação de medidas de segurança técnicas e administrativas aptas a proteger os dados de acessos não autorizados.

A acumulação massiva de dados pela máquina estatal, se desprovida de limites, transmuta-se numa ferramenta de monitoramento constante. A infraestrutura tecnológica de tratamento de dados do Estado atua, nesse sentido, como um verdadeiro panóptico moderno. No modelo panóptico, a visibilidade constante e a percepção de uma vigilância invisível garantem o funcionamento automático do poder e a submissão dos comportamentos. A posse e o cruzamento de informações pessoais pelo Estado ampliam esse mecanismo, estabelecendo uma anatomia política na qual o saber extraído do indivíduo serve para reforçar a sua sujeição. Assim, Foucault (1999) evidencia a relação entre vigilância, produção de saber e estruturação das relações de poder.

> Temos antes que admitir que o poder produz saber (e não simplesmente favorecendo-o porque o serve ou aplicando-o porque é útil); que poder e saber estão diretamente implicados; que não há relação de poder sem constituição correlata de um campo de saber, nem saber que não suponha e não constitua ao mesmo tempo relações de poder (Foucault, 1999, p. 31)

A utilização da categoria foucaultiana de panoptismo, neste trabalho, possui função analítica e não pretende estabelecer equivalência jurídica entre o modelo disciplinar descrito por Foucault e os atuais sistemas estatais de tratamento de

CC BY

RJNM
ISSN 2675-4312

Received: 13/10/2026 - **Accepted:** 11/11/2026
Vol: 07.11
DOI: 10.66104/29137t27
Pages: 1-18

dados. Serve, no entanto, para ilustrar como, na era digital, este campo de saber converteu-se em bases de dados e algoritmos preditivos.

Decisões administrativas baseadas em perfis algorítmicos podem produzir discriminação, falta de transparência e violação de direitos fundamentais. Quando os critérios de classificação permanecem inacessíveis, como em sistemas de negação automática de benefícios sociais, o cidadão pode não compreender os fundamentos da decisão nem identificar eventuais erros nos dados utilizados. Esse cenário contraria o princípio da não discriminação previsto no artigo 6º, inciso IX, da LGPD. Ademais, o artigo 20 da mesma lei assegura ao titular o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado. Esse risco materializa-se na automação da triagem e da concessão de benefícios previdenciários (como no INSS), onde a ausência de parâmetros acessíveis pode dificultar o exercício dos direitos de defesa.

A conciliação entre eficiência administrativa e proteção de dados exige políticas de governança e compartilhamento de informações que observem finalidades específicas, evitando que a interoperabilidade do Governo Digital resulte em cruzamento indiscriminado. Dessa forma, a proteção de dados deve estabelecer limites à atuação estatal, assegurando que eficiência e transparência administrativa sejam compatíveis com a privacidade.

6 O CONTROLO SOCIAL DA ADMINISTRAÇÃO PÚBLICA: TRANSPARÊNCIA E A LEI DE ACESSO À INFORMAÇÃO

A harmonização entre a proteção de dados e a transparência exige mais do que a simples edição de normas, demandando engajamento ativo da sociedade civil no controle das ações estatais. Na sociedade conectada, as redes interconectadas proporcionam novas dinâmicas de participação política e de articulação democrática, fenômeno estruturado pelo ciberativismo e pela cibercultura. Compreendendo que as tecnologias comunicacionais não são “meras ferramentas transparentes”, mas sim um “modelo global de organização do poder” (Martín-Barbero, 1997, p. 256), a

CC BY

RJNM
ISSN 2675-4312

Received: 13/10/2026 - **Accepted:** 11/11/2026
Vol: 07.11
DOI: 10.66104/29137t27
Pages: 1-18

consolidação democrática ancora-se na necessidade de disputar os imaginários e as configurações sociotécnicas que circulam na cultura jurídica e política brasileira. Essa apropriação do espaço digital permite à sociedade civil monitorar e intervir diretamente nas políticas públicas, transformando a profunda assimetria informacional do Estado em efetivo controle social.

> A tecnologia amplia a capacidade de participação social; cria nova escala de associação articuladora das redes sociais; e possibilita novas formas de organização política e da ação coletiva [...] A tecnologia tem como pressuposto a ação coletiva e direta dos seus membros, ou seja, os atores unem-se para potencializar as suas possibilidades de ação. (Egler, 2010, p. 232 *apud* Penteado; Araújo; Pimentel, 2012, p. 132).

Para que este controlo social seja efetivo e a Lei de Acesso à Informação (LAI) alcance a sua plenitude, a arquitetura tecnológica do Estado não pode operar como uma caixa negra inescrutável. A transparência pública pressupõe o escrutínio dos próprios sistemas que armazenam, processam e divulgam os dados dos cidadãos. Neste sentido, a adoção de padrões abertos e de *software* livre pela Administração Pública apresenta-se como uma exigência não apenas técnica, mas profundamente democrática. Silveira (2004) adverte que o conhecimento tecnológico deve ser partilhado para evitar a concentração de poder e assegurar a soberania popular:

> As tecnologias de informação e comunicação estão se consolidando como meios de expressão do conhecimento [...] Os protocolos de comunicação em rede e os softwares básicos [...] como meios de comunicação, precisam ser livres e desenvolvidos de maneira democrática e colaborativa. (Silveira, 2004, p. 42).

CC BY

RJNM
ISSN 2675-4312

Received: 13/10/2026 - **Accepted:** 11/11/2026
Vol: 07.11
DOI: 10.66104/29137t27
Pages: 1-18

A autonomia tecnológica proporcionada por padrões abertos garante que a sociedade civil e os órgãos de controlo auditem os algoritmos e as bases de dados governamentais, assegurando que a proteção da identidade digital não seja desvirtuada para ocultar informações de interesse público. Consequentemente, o desenvolvimento de sistemas nacionais de identidade digital e a crescente utilização de inteligência artificial pelo Estado exigem transparência algorítmica e a possibilidade de revisão humana, fortalecendo a *accountability* digital e a proteção contra discriminações ou opacidade sistémica.

O fortalecimento da Autoridade Nacional de Proteção de Dados (ANPD) e a consolidação de uma cultura de proteção de dados na Administração Pública são, portanto, passos fundamentais para que o Brasil avance na agenda digital sem retrocessos no campo dos direitos fundamentais. A verdadeira governação estabelece-se quando o sistema estatal é auditável e o seu funcionamento é transparente para os cidadãos, permitindo à sociedade exercer o seu direito de escrutínio ativo enquanto tem a sua privacidade rigorosamente preservada.

7 CONSIDERAÇÕES FINAIS

A análise desenvolvida demonstrou que a proteção de dados pessoais e a transparência administrativa constituem dimensões igualmente relevantes da proteção dos direitos fundamentais e da organização democrática do Estado. A elevação da proteção de dados pessoais ao rol dos direitos fundamentais, promovida pela Emenda Constitucional nº 115/2022, reforçou a necessidade de que o tratamento de informações pessoais pelo Poder Público observe parâmetros jurídicos de finalidade, adequação, necessidade, segurança e transparência.

A relação entre a Lei Geral de Proteção de Dados Pessoais e a Lei de Acesso à Informação não deve, portanto, ser compreendida a partir de uma oposição absoluta entre privacidade e publicidade. A aplicação de ambas as normas exige interpretação sistemática e consideração das circunstâncias concretas,

CC BY

RJNM
ISSN 2675-4312

Received: 13/10/2026 - **Accepted:** 11/11/2026
Vol: 07.11
DOI: 10.66104/29137t27
Pages: 1-18

especialmente da natureza da informação, da finalidade do tratamento, da existência de fundamento jurídico e da intensidade da interferência sobre os direitos do titular.

No âmbito da Administração Pública, informações pessoais diretamente relacionadas ao exercício da função pública podem estar sujeitas a regime de publicidade, desde que presentes fundamento jurídico, pertinência com a finalidade de transparência e observância dos princípios da necessidade e da proporcionalidade, preservando-se as informações relativas à esfera privada que não apresentem vínculo suficiente com o interesse público.

A análise jurisprudencial também evidencia que não é possível estabelecer consequências jurídicas uniformes para toda e qualquer situação de tratamento ou exposição indevida de dados pessoais. A natureza dos dados, a forma de tratamento, a existência de divulgação a terceiros, a finalidade da operação e a efetiva repercussão sobre os direitos da personalidade são elementos relevantes para a definição das consequências jurídicas aplicáveis.

No contexto da transformação digital da Administração Pública, a utilização de sistemas automatizados e o crescente compartilhamento de bases de dados ampliam a necessidade de mecanismos de governança, segurança, controle de acesso e responsabilização. O uso de categorias como “panóptico digital”, a partir da perspectiva foucaultiana, permite problematizar os riscos decorrentes da concentração informacional, sem que essa abordagem teórica seja confundida com uma categoria jurídica positivada.

Conclui-se, assim, que o desafio contemporâneo não consiste em escolher entre transparência e proteção de dados, mas em estabelecer critérios jurídicos capazes de compatibilizar ambas as dimensões. A transparência deve assegurar condições efetivas de controle da Administração Pública, enquanto a proteção de dados deve impedir tratamentos excessivos ou incompatíveis com as finalidades legítimas da atuação estatal. A adequada governança informacional constitui, nesse cenário, instrumento relevante para a conciliação entre publicidade administrativa, proteção da personalidade e funcionamento democrático das instituições.

CC BY

RJNM
ISSN 2675-4312

Received: 13/10/2026 - **Accepted:** 11/11/2026
Vol: 07.11
DOI: 10.66104/29137t27
Pages: 1-18

Referências

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2008.

ANPD – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo para o Poder Público: tratamento de dados pessoais pelo Poder Público**. Brasília, DF: ANPD, 2023.

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

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 2026.

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. Brasília, DF: Presidência da República, 2022.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, 2002.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal (Lei de Acesso à Informação). Brasília, DF: Presidência da República, 2011.

CC BY

RJNM
ISSN 2675-4312

Received: 13/10/2026 - **Accepted:** 11/11/2026
Vol: 07.11
DOI: 10.66104/29137t27
Pages: 1-18

BRASIL**. Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Brasília, DF: Presidência da República, 2014.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Ações Diretas de Inconstitucionalidade nº 6.387, 6.388, 6.389 e 6.390/DF**. Medida Provisória nº 954/2020. Compartilhamento de dados de usuários de telecomunicações com o IBGE. Reconhecimento da proteção de dados como direito fundamental. Relatora: Min. Rosa Weber, julgado em 7 maio 2020. Brasília, DF: STF, 2020.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário com Agravo nº 639.228/RJ.** Divulgação da remuneração de servidores públicos em sítio eletrônico oficial da Administração Pública. Repercussão Geral (Tema 483). Relator: Min. Luiz Fux, julgado em 2015. Brasília, DF: STF, 2015.

BRASIL. Superior Tribunal de Justiça (3ª Turma). **Recurso Especial nº 1.758.761/SP**. Relator: Ministro Marco Aurélio Bellizze. Julgado em: 08 set. 2020. Publicado no DJe em: 14 set. 2020.

BRASIL. Superior Tribunal de Justiça. **Informativo de Jurisprudência nº 817**. Brasília, DF: STJ, divulgado em 25 de junho de 2024

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão**. Tradução de Raquel Ramalhete. 20. ed. Petrópolis: Vozes, 1999.

MARTÍN-BARBERO, J. **Dos meios às mediações: comunicação, cultura e hegemonia**. Rio de Janeiro: Editora UFRJ, 1997.

CC BY

RJNM
ISSN 2675-4312

Received: 13/10/2026 - **Accepted:** 11/11/2026
Vol: 07.11
DOI: 10.66104/29137t27
Pages: 1-18

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 7. ed. rev. e atual. São Paulo: Saraiva, 2012.

PENTEADO, Cláudio Luis de Camargo; ARAÚJO, Rafael de Paulo Aguiar; SANTOS, Marcelo Burgos dos. *Sociedade civil e políticas públicas: o uso da internet pela Rede Nossa São Paulo na articulação política (2012)*. In: SILVEIRA, Sérgio Amadeu da; BRAGA, Sérgio; PENTEADO, Cláudio (org.). **Cultura, política e ativismo nas redes digitais**. 1. ed. São Paulo: Editora Fundação Perseu Abramo, 2014. p. 125-144.

SILVEIRA, Sérgio Amadeu da. **Software livre: a luta pela liberdade do conhecimento**. São Paulo: Editora Fundação Perseu Abramo, 2004.

CC BY