

O direito fundamental à privacidade nas cortes constitucionais do Brasil e da Argentina *The Fundamental Right to Privacy in the Constitutional Courts of Brazil and Argentina*

Andréa Nunes Melo¹

v. 14/n. 1 (2026)
Janeiro/Março

Aceito para publicação em 16/03/2026.

¹Doutoranda em Ciências Jurídicas pela Universidad del Museo Social Argentino, Buenos Aires, Argentina. ORCID: 0009-0001-7016-3580. E-mail: andreanunes23@hotmail.com.

RESUMO: O presente artigo discute o direito fundamental à privacidade a partir da atuação das Cortes Constitucionais do Brasil e da Argentina, em um contexto no qual dados pessoais, rastros digitais e mecanismos de vigilância alteram a forma como se produzem interferências na vida privada. Nessa ótica, o problema enfrentado está em identificar quais critérios o Supremo Tribunal Federal e a Corte Suprema de Justicia de la Nación utilizam para afirmar, restringir e proteger a privacidade diante de medidas estatais investigativas e administrativas e diante de práticas privadas de tratamento informacional, delimitando quando há justificativa legítima e quais salvaguardas precisam estar presentes. Com esse recorte, o objetivo é comparar padrões argumentativos, apontar convergências e diferenças e indicar consequências práticas para a tutela do direito em ambientes digitais, nos quais a intrusão pode ocorrer sem contato físico e em escala massiva. Para tanto, a metodologia adota abordagem qualitativa, com pesquisa bibliográfica e documental, combinando doutrina nacional e estrangeira com seleção de julgados paradigmáticos, escolhidos pela relevância da privacidade como razão decisória e pela densidade de fundamentação. No Brasil, discute-se a construção jurisprudencial em conflitos entre liberdade de expressão e direitos da personalidade, a recusa de um direito ao esquecimento como poder geral de apagamento e o aumento do ônus justificatório quando o Estado pretende coletar e compartilhar dados em larga escala, com ênfase em finalidade, necessidade e garantias. Na Argentina, analisam-se precedentes que protegem a esfera de reserva mesmo diante de notoriedade pública, além do desenvolvimento do *hábeas data* e do controle de intervenções em comunicações, inclusive com tutela coletiva quando a afetação é estrutural. Ao final, o trabalho sustenta que, embora os caminhos processuais e a linguagem jurídica variem, ambos os tribunais caminham para exigir legalidade, limites precisos e salvaguardas verificáveis como condição para restrições à privacidade no constitucionalismo contemporâneo.

Palavras-chave: Direito Constitucional; Constitucionalismo; Proteção de dados pessoais; Controle jurisdicional.

ABSTRACT: The present article examines the fundamental right to privacy through the lens of the Constitutional Courts of Brazil and Argentina, in a context in which personal data, digital traces, and surveillance mechanisms transform the ways in which interferences with private life occur. From this perspective, the central problem lies in identifying the criteria employed by the Brazilian Supreme Federal Court and the Argentine Supreme Court of Justice to affirm, restrict, and protect privacy in the face of investigative and administrative state measures, as well as private practices of informational processing, delimiting when legitimate justification exists and which safeguards must be ensured. Within this framework, the objective is to compare argumentative patterns, highlight convergences and divergences, and indicate practical consequences for the protection of the right in digital environments, where intrusion may occur without physical contact and on a massive scale. To this end, the methodology adopts a qualitative approach, based on bibliographic and documentary research, combining national and foreign doctrine with the selection of paradigmatic judicial decisions, chosen for the relevance of privacy as a decisive ground and for the density of their reasoning. In Brazil, the analysis addresses the jurisprudential construction in conflicts between freedom of expression and personality rights, the

<https://www.gvaa.com.br/revista/index.php/RDGP>

rejection of a right to be forgotten conceived as a general power of erasure, and the increase in the justificatory burden when the State seeks to collect and share data on a large scale, with emphasis on purpose, necessity, and safeguards. In Argentina, the article examines precedents that protect the sphere of reserve even in cases of public notoriety, as well as the development of habeas data and the control of interventions in communications, including collective remedies when the impact is structural. In conclusion, the study argues that, although procedural paths and legal language vary, both courts increasingly require legality, precise limits, and verifiable safeguards as conditions for restrictions on privacy within contemporary constitutionalism.

Keywords: Constitutional Law; Constitutionalism; Personal data protection; Judicial review.

1. CONSIDERAÇÕES INICIAIS

A privacidade, em sua trajetória contemporânea, é discutida como condição prática de liberdade, igualdade e desenvolvimento da personalidade em sociedades atravessadas por tecnologias de informação, circulação de dados e novas formas de vigilância. Ainda que a tradição liberal tenha oferecido bases duradouras para a defesa de uma esfera protegida, a discussão jurídica ganha notoriedade quando se reconhece que a exposição de informações pode produzir efeitos tão intensos quanto uma intervenção física, inclusive pela capacidade de traçar perfis, antecipar condutas e condicionar escolhas (Warren; Brandeis, 1890).

Nesta senda, a formulação do direito de estar só como reação a intromissões indevidas já indicava a necessidade de resposta jurídica a práticas sociais e tecnológicas emergentes. Em chave complementar, a privacidade também se consolida como linguagem de equilíbrio entre vida pública e vida privada, especialmente quando se compreende que a autodeterminação depende de um mínimo de controle sobre fluxos informacionais e sobre a circulação social de dados (Westin, 1967).

A passagem do debate da intimidade para a proteção de dados pessoais reorganiza o problema, pois se trata de disciplinar a coleta, o tratamento e o compartilhamento de informações em ambientes nos quais o dado se converte em insumo econômico e instrumento de governança. A partir dessa lente, a privacidade se aproxima de uma estrutura normativa voltada a limitar assimetrias de poder e a impor deveres de finalidade, necessidade e proporcionalidade no tratamento informacional.

Nessa linha, a proteção de dados é defendida como direito fundamental com lógica própria, ainda que em diálogo com a privacidade tradicional, justamente porque a ameaça reside na arquitetura de tratamento e na capacidade de reidentificação e cruzamento de bases (Rodotà, 2009).

Em consonância, Cruz e Camargo (2021), ao discutirem as medidas públicas de compartilhamento de informações em contexto de crise sanitária, explica como a tutela do dado exige critérios de precedência e condições de legitimidade que vão além de justificativas genéricas de interesse público.

Quando esse debate é deslocado para as Cortes Constitucionais do Brasil e da Argentina, o tema adquire feição institucional, tendo em vista que o que está em jogo é como tribunais de cúpula

controlam restrições, constroem padrões de motivação e definem limites a políticas estatais e práticas privadas que impactam a vida informacional.

No caso argentino, a discussão se ancora em tradição constitucional e convencional que confere relevo à *intimidad* e às garantias correlatas, exigindo que intervenções investigativas e medidas de coleta sejam submetidas a controles de legalidade e razoabilidade, com especial atenção à independência do controle e à calibragem do meio empregado (Campos, 2000). Já a Bernard (2021) demonstra como o avanço tecnológico amplia zonas de fricção entre poderes estatais e direitos, tornando pertinente o modo como o Judiciário examina autorização, extensão, finalidade e salvaguardas procedimentais (Bernard, 2021).

É nesse cenário que o presente artigo delimita como problema jurídico a identificação dos critérios empregados pelas Cortes Constitucionais do Brasil e da Argentina para afirmar, restringir e proteger o direito fundamental à privacidade, principalmente diante de práticas de tratamento de dados e de medidas estatais de natureza investigativa ou administrativa em ambiente digital.

Nesse âmbito, o objetivo desse artigo é analisar, de forma comparada, como o Supremo Tribunal Federal e a Corte Suprema de Justicia de la Nación constroem padrões argumentativos para controlar ingerências informacionais, buscando explicitar convergências, distinções e consequências práticas para a tutela do direito.

Para tanto, a metodologia adota abordagem qualitativa, com pesquisa bibliográfica e documental. No eixo bibliográfico, o levantamento foi realizado em bases de dados acadêmicas e repositórios jurídicos de ampla circulação, com busca concentrada em Scielo, Google Scholar, HeinOnline, JSTOR e SSRN, além de catálogos de editoras e bibliotecas digitais voltadas à doutrina constitucional e aos direitos fundamentais.

Para literatura latino-americana e ibero-americana, a pesquisa incluiu Dialnet e RedALyC, o que ampliou o acesso a estudos contemporâneos sobre o tema. A estratégia de busca combina descritores em português e espanhol, com variações em inglês quando necessário, empregando expressões como “direito à privacidade”, “intimidade”, “vida privada”, “sigilo das comunicações”, “proteção de dados pessoais”, “habeas data”, “Corte Suprema de Justicia de la Nación”, “Supremo Tribunal Federal”, “constitucionalismo digital” e “vigilância”, com operadores booleanos e filtros por título, resumo e palavras-chave.

O recorte temporal para a literatura científica priorizou publicações dos últimos dez anos, sem excluir obras clássicas e consolidadas indispensáveis à base teórica do tema, em especial quando são referência recorrente na construção dogmática do direito à privacidade e na delimitação de seu conteúdo normativo.

No eixo documental, o corpus jurisprudencial foi composto por decisões paradigmáticas do Supremo Tribunal Federal e da Corte Suprema de Justicia de la Nación, obtidas em repositórios oficiais e sistemas de consulta institucional, com preferência por acórdãos colegiados e decisões com maior densidade argumentativa, sem prejuízo de decisões individuais quando tiverem papel reconhecido na formação do entendimento do tribunal.

No caso brasileiro, a coleta considerou o portal do STF e mecanismos de pesquisa por classe processual, temas de repercussão geral e palavras-chave associadas a privacidade, intimidade, sigilo, dados pessoais, comunicações e tratamento informacional. No caso argentino, a coleta utilizou o Centro de Información Judicial e bases institucionais correlatas, com pesquisa por “intimidad”, “vida privada”, “datos personales”, “habeas data”, “interceptación”, “vigilancia” e “secreto”, além de termos vinculados à proteção constitucional e convencional.

A seleção dos julgados foi orientada por pertinência e capacidade de representar linhas decisórias, onde entraram no recorte decisões em que a privacidade aparece como razão determinante de decidir, seja para impor limites à atuação estatal, seja para estabelecer deveres de proteção e parâmetros de validade em face de riscos informacionais, excluindo-se casos em que a privacidade seja apenas como menção lateral, sem impacto real na fundamentação.

2. FUNDAMENTOS CONSTITUCIONAIS DO DIREITO À PRIVACIDADE NO BRASIL E NA ARGENTINA

A tutela constitucional da vida privada, tal como hoje se enuncia no vocabulário dos direitos fundamentais, nasceu de uma lenta sedimentação histórica que combina a proteção do espaço doméstico, a defesa da honra e a contenção do poder estatal sobre a circulação de informações pessoais. Ainda no século XIX, a percepção de que a exposição pública poderia produzir danos juridicamente relevantes levou à formulação de uma ideia estruturante, que é o fato da privacidade como esfera de resguardo contra intromissões indevidas, inclusive quando não há violência física, mas há captura e difusão de aspectos íntimos da existência humana (Warren; Brandeis, 1890).

Na tradição constitucional argentina, essa história ingressou pela porta das garantias clássicas do constitucionalismo liberal, em especial a inviolabilidade do domicílio e dos papéis privados, a proteção da correspondência e a exigência de legalidade estrita para medidas restritivas. O texto constitucional, ao consagrar limites ao poder de persecução e de vigilância, antecipou uma compreensão de privacidade como condição de liberdade, antes mesmo de empregar expressões contemporâneas vinculadas a dados pessoais, justamente porque a proteção recai, em primeiro plano, sobre a integridade do âmbito privado e sobre a vedação de ingerências arbitrárias (Argentina, 1994).

No percurso brasileiro, a proteção do segredo doméstico e das comunicações também apareceu antes de 1988, mas é a Constituição vigente que elevou o tema a uma posição mais explícita, ao enunciar a inviolabilidade da intimidade, da vida privada, da honra e da imagem, além de ampliar o sigilo de correspondência e das comunicações, inclusive no plano de dados e de comunicações telefônicas, sob reserva jurisdicional e nos termos da lei. Tal desenho constitucional limita a ação estatal e cria um parâmetro de validade para práticas privadas que atinjam a personalidade, ao vincular a proteção da esfera privada à responsabilização por danos e a um catálogo de garantias diretamente exigíveis (Brasil, 1988).

A passagem da história às categorias dogmáticas mostra que privacidade, intimidade e vida privada não são sinônimos perfeitos, ainda que convergentes na finalidade de assegurar uma zona de autodeterminação. No léxico constitucional brasileiro, a técnica de positivação mostra um núcleo mais reservado, frequentemente associado à intimidade, e um círculo mais amplo de vida privada, sem que isso autorize relativizações automáticas, pois o que se altera é o grau de exposição legítima e o tipo de interesse público capaz de justificar restrições, sempre sob controle de proporcionalidade e com preservação do conteúdo essencial do direito (Silva, 2013).

Com a sociedade informacional, o debate alcançou a circulação, o armazenamento e a recombinação de informações identificáveis, introduzindo uma agenda de proteção de dados pessoais que não se confunde com a privacidade clássica, embora se alimente dela. Nesse cenário, a privacidade permanece como direito de personalidade e como limite a interferências, todavia, a proteção de dados reorganiza o problema ao deslocar o foco para o ciclo de vida da informação pessoal, para o controle sobre o tratamento e para a prevenção de assimetrias entre titulares e agentes de tratamento (Doneda, 2006).

A Constituição argentina, reformada em 1994, dá um passo institucional importante ao inserir, ao lado do amparo, um mecanismo específico para acesso, retificação, atualização e confidencialidade de dados constantes de registros ou bancos de dados, públicos e privados destinados a fornecer informes, consolidando a ação de *hábeas data* como garantia conectada à tutela da intimidade e à governança de informações pessoais. Ao mesmo tempo, a reforma melhorou a arquitetura de abertura constitucional ao direito internacional dos direitos humanos, conferindo hierarquia constitucional a tratados selecionados, o que amplia o repertório normativo disponível para fundamentar e densificar o conteúdo do direito à privacidade (Argentina, 1994).

No plano infraconstitucional argentino, a Lei 25.326 complementou esse arranjo ao estruturar princípios, bases de licitude, direitos dos titulares e regras de funcionamento para bases de dados, além de disciplinar, em termos procedimentais, o exercício do *hábeas data* previsto constitucionalmente. Nesse ínterim, a proteção da vida privada, quando atravessada pela lógica do

tratamento automatizado e do uso econômico de informações, passou a ser operacionalizada por um regime jurídico que busca ordenar a coleta e o uso de dados, estabelecer limites e criar instrumentos de controle e reparação (Argentina, 2000).

No Brasil, a resposta normativa seguiu outra trilha. A Constituição de 1988 apresentou de início o fundamento geral, e a Lei Geral de Proteção de Dados introduziu um sistema de princípios e direitos que conectou a tutela de dados a valores constitucionais, como liberdade, privacidade e desenvolvimento da personalidade, sem abandonar as garantias tradicionais de sigilo e reserva (Brasil, 1988).

A LGPD, ao definir conceitos, hipóteses de tratamento e deveres de governança, atua como ponte entre o catálogo constitucional e as práticas contemporâneas de processamento informacional, tornando juridicamente rastreáveis os riscos que antes eram percebidos apenas como exposição ou devassa (Brasil, 2018).

A positivação constitucional brasileira evoluiu ainda mais quando a proteção de dados pessoais passou a ser explicitada no texto constitucional, tanto como direito fundamental quanto como matéria sujeita a competência normativa federal, indicando uma escolha institucional por uniformidade regulatória e por maior densidade de tutela no patamar constitucional. Tal movimento não substitui o art. 5º, X, nem as garantias de sigilo do art. 5º, XII, não obstante, ele reorganizou a leitura do sistema ao reconhecer que o risco contemporâneo inclui o uso contínuo e massificado de informações pessoais em infraestruturas digitais e administrativas (Brasil, 2022).

A doutrina abalizada tende a registrar que, no citado país, a proteção de dados se consolidou como eixo próprio sem perder a filiação à privacidade, e que essa filiação se espelha na forma pela qual o sistema interpreta dados sensíveis, consentimento, finalidade e discriminação, sempre sob a ideia de que certos tratamentos produzem riscos diretos à personalidade e à igualdade material. Nessa perspectiva, a proteção constitucional e legal ganha massa volumar quando se observa que a privacidade é um campo de contenção de vulnerabilidades produzidas por coleta e uso indevido de informações pessoais (Sarlet; Ruaro, 2021).

Ao comparar as estruturas constitucionais, nota-se que o Brasil adota um modelo mais enumerativo e textualizado na declaração de direitos, o que facilita o enquadramento imediato de conflitos em torno de intimidade e vida privada, enquanto a Argentina combina cláusulas de proteção individual, garantias processuais e remédios constitucionais aptos a operar como vias de concretização, com forte diálogo com tratados de direitos humanos e com o desenvolvimento jurisprudencial de princípios.

Para Sagüés (2007), a diferença pode repercutir na forma de argumentar, no caminho processual escolhido e na maneira pela qual o sistema acolhe novos problemas, como vigilância,

bancos de dados e perfilamento. Outrossim tal tema se desarticula da intimidade clássica para uma tutela estruturada por direitos de acesso, correção e controle, sem abandonar a matriz constitucional que confere legitimidade e direção ao sistema (Peruzzotti, 2024).

Nesse desenho comparado, os tratados de direitos humanos agem como matriz comum, mormente no sistema argentino após 1994, e como referência interpretativa também no Brasil, ainda que por mecanismos distintos de incorporação e hierarquia. A Convenção Americana, ao enunciar a vedação de interferências arbitrárias ou abusivas na vida privada, na família, no domicílio e na correspondência, apresenta uma linguagem normativa que aproxima intimidade e integridade informacional e serve de parâmetro para justificar restrições estatais e deveres de proteção em face de atores privados, o que se torna importante em contextos digitais (OEA, 1969).

3. A CONSTRUÇÃO JURISPRUDENCIAL DO DIREITO À PRIVACIDADE NAS CORTES CONSTITUCIONAIS

Inicialmente, é possível afirmar que o entendimento firmado pelos tribunais sobre o direito à privacidade nas Cortes Constitucionais brasileira e argentina possibilita compreender a trajetória interpretativa que acompanha mudanças de época. Primeiro, o embate clássico entre imprensa e vida privada, depois a expansão do poder investigativo e, mais recentemente, a transição para litígios em que dados, rastros digitais e formas difusas de vigilância modificam o próprio conteúdo protegido.

A história comum, porém, não elimina diferenças relevantes, considerando que o Supremo Tribunal Federal (STF) tende a explicitar critérios de ponderação em chave de proporcionalidade, enquanto a Corte Suprema de Justicia de la Nación (CSJN) consolidou, em certos marcos, padrões argumentativos fortemente vinculados ao desenho institucional do amparo e da tutela coletiva, além da tradição de esfera de reserva que limita o olhar público e estatal sobre o indivíduo (Argentina, 1984).

No itinerário brasileiro, um ponto de mudança frequentemente citado é o julgamento das biografias não autorizadas, no qual o STF foi chamado a definir, sem eufemismos, a fronteira entre tutela da personalidade e interdição prévia do discurso público, reconhecendo que a proteção da privacidade não pode ser instrumentalizada como mecanismo de controle antecipado de circulação de ideias, ao mesmo tempo em que preservou, no plano subsequente, a possibilidade de responsabilização civil quando presentes abusos e danos. O que se destaca, para além do resultado, é o método, visto que o Tribunal enfrenta o conflito como colisão entre direitos, recusa hierarquias abstratas e procura delimitar a incidência legítima de restrições, deslocando a privacidade para um

terreno em que ela atua mais como parâmetro de responsabilização e de tutela posterior do que como autorização para barreiras prévias ao debate público (Brasil, 2015).

Essa mesma lógica de evitar soluções que funcionem como veto estrutural à circulação de informações aparece, com formulação própria, no julgamento em que o STF fixou entendimento sobre a incompatibilidade constitucional de um direito ao esquecimento concebido como poder geral de impedir a divulgação de fatos verídicos e lícitamente obtidos apenas pela passagem do tempo.

O referido Tribunal, ao negar provimento ao RE 1.010.606/RJ, não negou a existência de situações de sofrimento e estigmatização, não obstante, rejeitou a criação de uma categoria com pretensão de bloquear, em abstrato, registros e narrativas, transferindo o foco para o exame do caso concreto por meio de parâmetros já existentes, como eventuais excessos, violações de personalidade e ilicitudes específicas, e, assim, reafirmando uma compreensão de privacidade que opera mais como limite qualificado do que como direito de apagamento generalizado da memória social (Brasil, 2021).

Se, nos casos ligados à comunicação pública, a Corte brasileira preferiu conter categorias amplas que poderiam produzir censura indireta, no campo informacional ela aumentou as exigências de finalidade, necessidade e proteção efetiva contra riscos de uso indevido, especialmente quando o Estado pretende tratar dados em escala. A suspensão da eficácia da Medida Provisória n. 954/2020, no conjunto de ações diretas que tiveram como núcleo o compartilhamento de dados de usuários de telecomunicações para fins estatísticos, mostra uma virada discursiva, em que a privacidade passou a ser tratada como limite material à captura e circulação massiva de dados, exigindo justificativas verificáveis, salvaguardas técnicas e garantias institucionais de contenção do risco, sob pena de o tratamento estatal degenerar em coleta ampla e pouco controlável (Brasil, 2020).

A relevância desse conjunto decisório está em explicitar um padrão de controle, onde a Corte examina a densidade normativa da finalidade, o desenho de governança, a minimização do dado e a possibilidade real de auditoria, fazendo com que o ônus argumentativo do Estado aumente quando a intervenção atinge a esfera informacional de milhões de pessoas.

É por isso que parte da doutrina passou a tratar esse julgamento como marco para compreender a privacidade em sua dimensão informacional, chamando atenção para o modo como o STF articulou, no raciocínio, a proteção de dados com o núcleo de direitos da personalidade e com garantias constitucionais de sigilo, sem depender de fórmulas genéricas e sem reduzir o problema a uma disputa abstrata entre eficiência administrativa e direitos individuais (Furtado; Bezerra, 2023).

Na Argentina, por sua vez, a CSJN construiu bases jurisprudenciais da privacidade em diálogo permanente com a tensão entre interesse público e esfera íntima, e o precedente “*Ponzetti de Balbín*” permanece emblemático porque formula que a notoriedade de uma pessoa não dissolve a reserva de

sua vida privada, nem autoriza a exploração de imagens e situações que pertencem ao núcleo de intimidade, sobretudo em circunstâncias de vulnerabilidade.

O que importa, metodologicamente, é que a Corte não se limita a afirmar a privacidade como valor moral, posto que ela vincula a proteção à ideia de que nenhum direito opera sem limites e que a liberdade de informar, quando desconectada de interesse público legítimo e de regularidade no exercício, pode converter-se em violação indenizável da esfera pessoal (Argentina, 1984).

Com a reforma constitucional de 1994 e a positivação expressa do *hábeas data*, a CSJN passou a enfrentar a privacidade também como direito de controle sobre informações pessoais. No caso “*Urteaga*”, a Corte afirmou que o acesso a registros e arquivos estatais integra a proteção da identidade e da esfera pessoal, impondo ao Estado deveres de transparência em relação ao que ele sabe sobre o indivíduo e reconhecendo que, sem essa via, a pessoa permanece exposta à produção e circulação de dados que podem afetar sua vida sem possibilidade real de correção ou esclarecimento. Nessa ótica, a privacidade possui contornos de tutela ativa, conectada à proteção da identidade e ao controle do indivíduo sobre dados existentes em arquivos públicos (Argentina, 1998).

Já o precedente “*Halabi*” consolidou outro elemento, o da privacidade como limite à vigilância e à intervenção em comunicações, ao mesmo tempo em que desenvolveu uma arquitetura de tutela que ultrapassa o caso individual quando a afetação assume caráter estrutural. A CSJN, invalidou dispositivos ligados à intervenção e retenção de dados de comunicações sem parâmetros suficientes, assim, aumentando a exigência de legalidade estrita e de limites precisos para interferências estatais, e, adicionalmente, estruturou a compreensão de que há situações em que a tutela judicial precisa alcançar uma coletividade de afetados para ser efetiva. O padrão argumentativo, assim sendo, combina reserva individual, legalidade e eficácia da jurisdição, evitando que violações sistêmicas sobrevivam por fragmentação processual (Argentina, 2009).

O ambiente digital trouxe, em seguida, disputas em que a privacidade se cruza com circulação de conteúdos e responsabilidade de intermediários, e o caso “*Rodríguez c/ Google*” é ilustrativo porque a CSJN enfrentou, sem legislação específica de responsabilidade de intermediários, a tensão entre proteção da personalidade e funcionamento de mecanismos de busca, definindo critérios para atribuição de responsabilidade e para ordens de remoção.

Ainda que o objeto imediato fosse responsabilidade civil, a Corte discutiu a tutela de direitos personalíssimos diante de associações prejudiciais, estabelecendo distinções que procuram evitar a indiferença diante de violações e a criação de deveres gerais de monitoramento incompatíveis com a liberdade de expressão e com a estrutura técnica da rede (Argentina, 2014).

A evolução posterior mostrou que a CSJN também foi provocada a tratar pedidos de desindexação e supressão de resultados de busca ligados a fatos de interesse público, e o julgamento

“*Denegri c/ Google*” recolocou o problema em outro patamar. A Corte avaliou o sentido de manter acessíveis registros audiovisuais e jornalísticos de acontecimentos com relevância pública, resistindo a soluções que produzam apagamento informacional de eventos históricos, especialmente quando vinculados ao debate público e à memória coletiva. O diálogo com a privacidade, nesse julgado, mais como critério para distinguir o que é mera curiosidade exploratória do que se mantém sob interesse público, exigindo argumentação demonstrável para medidas de supressão (Argentina, 2022).

4. DESAFIOS CONTEMPORÂNEOS À PROTEÇÃO DA PRIVACIDADE NO CONSTITUCIONALISMO BRASILEIRO E ARGENTINO

Conforme discutido ao longo do artigo, a passagem da privacidade do segredo para a privacidade como problema de governança, hoje, é impulsionada por um tipo de circulação de dados que não depende de sua conversão cotidiana em traços, como cliques, deslocamentos, interações, preferências e padrões inferidos.

Nesse ambiente, a tutela constitucional enfrenta modelos de coleta e predição que operam de forma contínua, muitas vezes invisível, produzindo assimetrias informacionais capazes de condicionar escolhas sem recorrer a coerção direta, o que reabre, em novos termos, a tensão entre autonomia e poder na sociedade digital (Zuboff, 2019).

Tal deslocamento afeta o modo como as Cortes Constitucionais justificam limites ao Estado e ao setor privado, porque a privacidade, diante de tecnologias de rastreamento, deixa de ser somente um direito de estar só e adota feição estrutural, tratando-se de impedir que o sujeito seja permanentemente transformado em objeto de observação e classificação. A vigilância contemporânea, ao combinar sensores urbanos, plataformas e bancos de dados interoperáveis, altera a própria ideia de esfera privada, já que o que se protege é a possibilidade de que a vida social não seja integralmente traduzida em dados tratáveis e recombinaíveis (Lyon, 2018).

No constitucionalismo brasileiro, o debate tecnológico se adensa porque a proteção da privacidade é testada hoje em situações de alto impacto institucional, nas quais o Estado pretende integrar, cruzar e reutilizar grandes conjuntos de dados para fins administrativos e regulatórios. Ao examinar o Decreto nº 10.046/2019 (Cadastro Base do Cidadão) e seus mecanismos de compartilhamento, o Supremo Tribunal Federal foi levado a tratar da compatibilidade entre eficiência administrativa e garantias constitucionais, fixando balizas que recolocam a privacidade como parâmetro para desenho institucional e não tão-somente como defesa reativa contra intromissões episódicas (Brasil, 2022).

Ainda no Brasil, o contencioso de dados também se projeta sobre a persecução penal e a inteligência financeira, em que o argumento da segurança tende a pressionar os limites do sigilo. No Tema 990 da repercussão geral (RE 1.055.941), o Supremo enfrentou o problema do compartilhamento de informações pela unidade de inteligência financeira e pela administração tributária com órgãos de investigação, em um cenário em que o dado é matéria-prima de triagens automatizadas e correlações, exigindo do Tribunal uma justificativa que trate da finalidade, do modo de circulação e das salvaguardas contra abusos (Brasil, 2019).

A fricção é ainda mais sensível quando a prova nasce de dispositivos digitais e de seus conteúdos armazenados, pois a distinção entre objeto e histórico de vida praticamente se dissolve em um *smartphone*. No Tema 977, ao reconhecer a ilicitude do acesso a dados armazenados em celular encontrado sem autorização judicial, o Supremo recoloca a privacidade no centro do devido processo em ambiente informacional, sinalizando que a disponibilidade fática do dispositivo não equivale a disponibilidade jurídica de seus conteúdos, especialmente quando a devassa permite reconstruir redes, rotinas e preferências com elevado poder intrusivo (Brasil, 2025).

No plano das cidades e das infraestruturas digitais, os desafios se ampliam com tecnologias de reconhecimento facial e outras formas de identificação biométrica, que tendem a normalizar a vigilância em tempo real e a triagem de pessoas em espaços públicos e privados. Sobre essa questão, Dal Magro e Fortes (2021) tem explicado que, mesmo quando apresentadas como medidas de segurança, essas soluções aumentam riscos de discriminação, ampliam o alcance do controle social e mudam o debate constitucional para temas como proporcionalidade, minimização, transparência e responsabilização, de maneira especial quando o tratamento se baseia em bases massivas e interoperáveis.

A esse quadro se soma, no Brasil, a maturação do regime legal de proteção de dados, que fornece vocabulário normativo para tratar de riscos típicos do ecossistema digital, como finalidade, necessidade, adequação, segurança, responsabilização e, por consequência, influencia a forma como a privacidade é argumentada em chave constitucional.

A Lei nº 13.709/2018, ao estruturar o tratamento de dados pessoais como atividade que exige fundamento, limites e deveres, tende a deslocar o debate jurídico de “se” pode coletar para “como”, “para quê” e “com quais garantias”, o que melhora a leitura da privacidade como direito a ser protegido por desenho normativo e institucional (Brasil, 2018).

Já no constitucionalismo argentino, a centralidade das novas tecnologias aparece em disputas sobre conteúdo online e em controvérsias de *hábeas data* que envolvem circulação de informações em redes e a definição de competência como condição de efetividade da tutela. No caso “*Ayala, Andrea Fabiana c/ Banco de Servicios y Transacciones S.A. s/ hábeas data*”, a Corte Suprema de

Justicia de la Nación reafirmou a excepcionalidade da competência federal prevista na Lei 25.326, vinculando-a a hipóteses específicas, como bases públicas de informação ou redes interjurisdicionais, o que mostra como, em litígios de dados, a arquitetura processual também é parte da proteção material, especialmente quando a informação transita por ambientes digitais que podem sugerir, nem sempre corretamente, uma dimensão interjurisdicional (Argentina, 2025).

A base normativa argentina, por sua vez, impõe que a leitura constitucional da privacidade dialogue com um regime legal de dados pessoais já consolidado e com disputas contemporâneas sobre adequação institucional frente a tecnologias emergentes, como *profiling*, decisões automatizadas e monitoramento em larga escala. A Lei 25.326, ao prever direitos de acesso, retificação e supressão e ao disciplinar bancos de dados, atua na concretização do art. 43 da Constituição (*hábeas data*), e acaba servindo de referência para calibrar, em ambiente digital, o equilíbrio entre inovação, consumo, crédito, segurança e autodeterminação informativa (Argentina, 2000).

Nesse contexto comparado, os desafios contemporâneos à privacidade envolvem a capacidade de STF e CSJN de manter coerência argumentativa quando enfrentam, de um lado, pretensões estatais de interoperabilidade e investigação orientada por dados e, de outro, ecossistemas privados baseados em extração, classificação e monetização de informações pessoais.

O ponto de fricção mais constante é que a tecnologia desloca a privacidade do plano individual para o plano sistêmico, exigindo decisões que tratem de riscos de longo prazo, incentivos institucionais e salvaguardas verificáveis, sob pena de a tutela constitucional perder densidade justamente onde a intrusão é mais escalável (Basterra, 2024).

5. CONSIDERAÇÕES FINAIS

A comparação entre o Supremo Tribunal Federal e a Corte Suprema de Justicia de la Nación mostrou que a privacidade hoje é uma regra de contenção do poder em ambientes de extração permanente de dados. Quando o Estado ou atores privados transformam rotinas em informação tratável, a violação já não depende de arrombamento, escuta clandestina ou exposição escandalosa, podendo ocorrer por integração silenciosa de bases, por retenção desmedida, por inferências automatizadas e por decisões tomadas a partir de perfis.

Diante disso, as Cortes também julgam a legitimidade de arquiteturas de vigilância, a qualidade das salvaguardas e a seriedade das justificativas apresentadas para a coleta e o compartilhamento, maiormente quando medidas aparentemente neutras atingem milhões e criam riscos duradouros.

Ainda assim, o estudo mostra que Brasil e Argentina percorrem caminhos próprios para chegar a exigências semelhantes. No Brasil, o STF tende a operar com uma gramática de colisão de direitos e de controle por proporcionalidade, ora refreando categorias que funcionariam como veto prévio à circulação de ideias, ora elevando o nível de exigência quando o tema é tratamento massivo de dados e governança institucional.

Na Argentina, a CSJN se apoia com mais frequência em uma tradição de esfera de reserva, no desenho do amparo e do *hábeas data* e na ideia de que violações sistêmicas exigem resposta jurisdicional capaz de alcançar a coletividade afetada, evitando que a proteção se fragmente em litígios isolados. O resultado é que, embora a linguagem e o caminho processual variem, ambas as Cortes projetam um recado comum, em que a privacidade é parâmetro de validade para políticas públicas e para práticas privadas, e sua restrição exige limites objetivos, motivação densa e mecanismos verificáveis de controle.

Logo, a conclusão que se impõe é que a a proteção da privacidade, na era digital, será tão forte quanto forem os freios colocados na engrenagem que coleta, retém, cruza e monetiza informações. O desafio contemporâneo é impedir que ele seja esvaziado por soluções vagas, por exceções em nome de segurança ou eficiência e por modelos técnicos que tornam a intrusão escalável e invisível.

Se STF e CSJN pretendem manter a privacidade como direito efetivo, precisarão continuar exigindo desenho normativo claro, governança responsável, minimização de dados, transparência real e responsabilização quando houver abuso, sob pena de a vida informacional se tornar um território sem limites, em que a liberdade se reduz ao que os sistemas permitem que o indivíduo seja.

REFERÊNCIAS

ARGENTINA. **Constitución de la Nación Argentina**. Buenos Aires: Ministerio de Justicia y Derechos Humanos, s.d. Disponível em: https://www.argentina.gob.ar/sites/default/files/derechoshumanos_publicaciones_colecciondebolsillo_01_constitucion_nacion_argentina.pdf. Acesso em: 17 jan. 2026.

ARGENTINA. Corte Suprema de Justicia de la Nación. **Ayala, Andrea Fabiana c/ Banco de Servicios y Transacciones S.A. s/ hábeas data (art. 43 C.N.)**. Fallos 348:295. Sentencia: 8 mayo 2025. Buenos Aires: CSJN, 2025. Disponível em: <https://sj.csjn.gov.ar/homeSJ/notas/nota/204/documento>. Acesso em: 17 jan. 2026.

ARGENTINA. **Corte Suprema de Justicia de la Nación**. Denegri, _____ c/ Google Inc. s/ derechos personalísimos: Acciones relacionadas (CIV 50016/2016/CS1). Buenos Aires, 28 jun. 2022. Disponível em: <https://repositorio.mpd.gov.ar/documentos/Denegri%20%28Causa%20n%C2%B050016%29.pdf>. Acesso em: 17 jan. 2026.

ARGENTINA. Corte Suprema de Justicia de la Nación. **Halabi, Ernesto c/ P.E.N. – ley 25.873 – dto. 1563/04 s/ amparo ley 16.986**. Buenos Aires, 24 feb. 2009. Disponível em: <https://www.saij.gob.ar/corte-suprema-justicia-nacion-federal-ciudad-autonoma-buenos-aires-halabi-ernesto-pen-ley-25783-dto-1563-04-amparo-ley-16986-fa09000006-2009-02-24/123456789-600-0009-0ots-eupmocsollaf>. Acesso em: 17 jan. 2026.

ARGENTINA. Corte Suprema de Justicia de la Nación. **Indalia Ponzetti de Balbín c/ Editorial Atlántida S.A. s/ daños y perjuicios**. Buenos Aires, 11 dic. 1984. Disponível em: https://www.saij.gob.ar/jurisprudencia/FA84000564-indalia_editorial_danos-federal-1984.htm. Acesso em: 17 jan. 2026.

ARGENTINA. Corte Suprema de Justicia de la Nación. **Rodríguez, María Belén c/ Google Inc. y otro s/ daños y perjuicios**. Buenos Aires, 28 oct. 2014. Disponível em: <https://www.saij.gob.ar/corte-suprema-justicia-nacion-federal-ciudad-autonoma-buenos-aires-rodriguez-maria-belen-google-inc-otro-danos-perjuicios-fa14000161-2014-10-28/123456789-161-0004-1ots-eupmocsollaf>. Acesso em: 17 jan. 2026.

ARGENTINA. Corte Suprema de Justicia de la Nación. **Urteaga, Facundo Raúl c/ Estado Nacional – Estado Mayor Conjunto de las FF.AA. s/ amparo ley 16.986. Fallos: 321:2767**. Buenos Aires, 15 oct. 1998. Disponível em: <https://www.saij.gob.ar/corte-suprema-justicia-nacion-federal-ciudad-autonoma-buenos-aires-urteaga-facundo-raul-estado-nacional-estado-mayor-conjunto-ffaa-amparo-ley-16986-fa98001242-1998-10-15/123456789-242-1008-9ots-eupmocsollaf>. Acesso em: 17 jan. 2026.

ARGENTINA. **Ley 25.326**, de 4 de octubre de 2000. Protección de los datos personales. Boletín Oficial de la República Argentina, Buenos Aires, 2 nov. 2000. Disponível em: <https://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/647/norma.htm>. Acesso em: 17 jan. 2026.

BASTERRA, Marcela I. **Derechos fundamentales en la era digital: privacidad, datos personales y desafíos institucionales**. 2024.

BERNARD, Jesica. Equilibrio entre el derecho a la intimidad y el poder investigativo del Estado en la era digital. **Revista Jurídica de la Universidad de Palermo**, Buenos Aires, ano 19, n. 2, p. 33-62, nov. 2021.

BIDART CAMPOS, Germán J. **Manual de la Constitución reformada**. Buenos Aires: Ediar, 2000.

BIDART CAMPOS, Germán J. **Tratado elemental de derecho constitucional argentino**. Buenos Aires: Ediar, 2000.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 17 jan. 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 e para fixar a competência privativa da União para legislar sobre a matéria. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 17 jan. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 jan. 2026.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6.649/DF; Arguição de Descumprimento de Preceito Fundamental nº 695/DF.** Relator: Min. Gilmar Mendes. Julgamento: 15 set. 2022. Diário da Justiça Eletrônico, Brasília, DF, 19 jun. 2023. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978491&ext=.pdf>; <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978671&ext=.pdf>. Acesso em: 17 jan. 2026.

BRASIL. Supremo Tribunal Federal. **Repercussão Geral. Tema 990. Recurso Extraordinário nº 1.055.941/SP** (compartilhamento de dados para fins de investigação). Relator: Min. Dias Toffoli. Julgamento: 4 dez. 2019. Diário da Justiça Eletrônico, Brasília, DF, 6 out. 2020. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=755364496>. Acesso em: 17 jan. 2026.

BRASIL. Supremo Tribunal Federal (Plenário). **Repercussão Geral. Tema 977. Agravo em Recurso Extraordinário nº 1.042.075/RJ** (acesso a dados armazenados em aparelho celular e necessidade de autorização judicial). Relator: Min. Dias Toffoli. Julgamento: 25 jun. 2025. Publicação: 24 set. 2025. Brasília, DF: STF, 2025. Disponível em: https://www.stf.jus.br/arquivo/cms/informativoInformativoSociedade/anexo/InformativoSociedadeStf_120.pdf. Acesso em: 17 jan. 2026.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade n. 4.815/DF.** Relatora: Ministra Cármen Lúcia. Tribunal Pleno. Julgamento em 10 jun. 2015. Publicação DJe em 1 fev. 2016. Disponível em: <https://noticias.stf.jus.br/postsnoticias/voto-da-ministra-carmen-lucia-afasta-exigencia-de-autorizacao-para-biografias/>. Acesso em: 17 jan. 2026.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade n. 6.387 MC-Ref/DF.** Relatora: Ministra Rosa Weber. Tribunal Pleno. Julgamento em 7 maio 2020. Disponível em: <https://www.lexml.gov.br/urn/urn:lex:br:supremo.tribunal.federal;plenario:acordao;adi:2020-05-07;6387-5898078>. Acesso em: 17 jan. 2026.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário n. 1.010.606/RJ (Tema 786).** Relator: Ministro Dias Toffoli. Tribunal Pleno. Julgamento em 11 fev. 2021. Disponível em: <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=460414>. Acesso em: 17 jan. 2026.

CUNHA E CRUZ, Marco Aurélio Rodrigues da; CAMARGO, Luís Henrique Kohl. O direito fundamental à proteção de dados pessoais e as condições de precedência em três medidas não farmacológicas adotadas pelo Brasil no enfrentamento da Covid-19. **Revista Eletrônica do Curso de Direito da UFSM**, Santa Maria, RS, v. 16, n. 1, e48479, 2021.

DAL MAGRO, Ana Flávia; FORTES, Pedro Rubim Borges. O reconhecimento facial e a segurança pública nas smart cities brasileiras: um debate sobre eficiência e direitos humanos. **Revista Direito Internacional**, Brasília, v. 18, n. 3, 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

FURTADO, Gabriel Rocha; BEZERRA, Daniel Teixeira. A (in)constitucionalidade da Medida Provisória nº 954/2020 no julgamento da ADI 6387: o marco jurisprudencial brasileiro do direito fundamental à proteção de dados pessoais. **Revista Eletrônica de Direito Civil (Civilistica.com)**, Rio de Janeiro, v. 12, n. 1, 2023.

LYON, David. **The culture of surveillance**: watching as a way of life. Cambridge: Polity Press, 2018.

OEA. **American Convention on Human Rights (“Pact of San José, Costa Rica”)**. 22 nov. 1969. Disponível em: https://www.oas.org/dil/treaties_b-32_american_convention_on_human_rights.pdf. Acesso em: 17 jan. 2026.

ONU. **International Covenant on Civil and Political Rights**. 16 dez. 1966. Disponível em: <https://www.ohchr.org/sites/default/files/ccpr.pdf>. Acesso em: 17 jan. 2026.

PERUZZOTTI, Mariano. Actualidad en materia de protección de datos personales en Argentina. **Cuadernos del Centro de Estudios de Diseño y Comunicación**, Buenos Aires, n. 217, p. 191-203, 2024.

RODOTÀ, Stefano. Data protection as a fundamental right. In: GUTWIRTH, Serge et al. (ed.). **Reinventing data protection?** Dordrecht: Springer, 2009. p. 77-82.

SÁ, M. I. O fundamento do direito ao esquecimento encontra-se na privacidade: reflexões a partir da jurisprudência constitucional brasileira. **Revista Brasileira de Direito Civil**, v. 28, p. 1-14, 2021.

SAGÜÉS, Néstor Pedro. **Manual de derecho constitucional**. 1. ed. Buenos Aires: Astrea, 2007.

SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – L. 13.709/2018. **Revista Direitos Fundamentais & Democracia**, Curitiba, v. 26, n. 2, p. 81-106, maio/ago. 2021.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 36. ed. São Paulo: Malheiros, 2013.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, Cambridge, v. 4, n. 5, p. 193-220, 15 dez. 1890.

WESTIN, Alan F. **Privacy and freedom**. New York: Atheneum, 1967.

ZUBOFF, Shoshana. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. New York: PublicAffairs, 2019.