Revista Brasileira de Direito e Gestão Pública
www.gvaa.com.br/revista/index.php/RDGP/
ISSN: 2358-2405

Proteção de dados pessoais como limite material ao poder de vigilância estatal

Protection of personal data as a material limit to the power of state surveillance

Andréa Nunes Melo[1]

v. 14/ n. 1 (2026)
Janeiro/Março

Aceito para publicação em 16/03/2026.

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

https://www.gvaa.com.br/revista/index.php/RDG

RESUMO: O presente artigo tem como base a mudança histórica da vigilância estatal, que passou a se estruturar no ambiente digital como capacidade contínua de coleta, correlação e inferência a partir de rastros informacionais, com impacto direto sobre a vida privada e sobre a distribuição social de suspeições. A partir desse diagnóstico, sustenta-se que a proteção de dados pessoais oferece ao constitucionalismo contemporâneo uma gramática própria para controlar o poder de vigilância, ao mover o debate do segredo para a legitimidade do tratamento, com exigências de finalidade, necessidade, limitação temporal, governança e responsabilidade institucional. Nesse ínterim, o objetivo é identificar parâmetros constitucionais e dogmáticos aptos a orientar o controle de práticas estatais de monitoramento e de bancos de dados voltados à segurança pública, tratando a proteção de dados como limite material à expansão silenciosa de escopos e ao reuso contínuo de informações por diferentes órgãos. Para tanto, a metodologia é bibliográfica e documental, de natureza jurídico-dogmática, com abordagem qualitativa e emprego de raciocínio dedutivo, partindo de premissas constitucionais sobre limites ao poder estatal e direitos fundamentais para extrair critérios aplicáveis a políticas de monitoramento e integração de bases. Outrosim, adota-se recorte temporal prioritário entre 2015 e 2025, com inclusão de obras formadoras indispensáveis, e revisão em repositórios como SciELO, RedALyC, HeinOnline, SSRN e Google Scholar. No plano das discussões, o texto delimita categorias jurídicas, como privacidade, intimidade, sigilo e autodeterminação informativa, examina riscos de perfilização e seletividade em ecossistemas de dados e organiza um padrão de controle constitucional baseado em legalidade estrita, proporcionalidade, minimização e retenção, reserva de jurisdição quando cabível, transparência compatível com segurança e mecanismos de auditabilidade e contestação, dialogando ainda com marcos normativos e institucionais do Brasil e da Argentina.

Palavras-chave: Direito Constitucional; Autodeterminação informativa; Vigilância informacional; Interoperabilidade.

ABSTRACT: This article is grounded in the historical transformation of state surveillance, which has come to be structured in the digital environment as a continuous capacity for collection, correlation, and inference based on informational traces, with direct effects on private life and on the social distribution of suspicion. From this diagnosis, it is argued that the protection of personal data provides contemporary constitutionalism with its own grammar for controlling surveillance power, by shifting the debate from secrecy to the legitimacy of data processing, with requirements of purpose, necessity, temporal limitation, governance, and institutional accountability. In this context, the objective is to identify constitutional and doctrinal parameters capable of guiding the control of state monitoring practices and security-oriented databases, treating data protection as a material limit to the silent expansion of scopes and to the continuous reuse of information by different public bodies. To this end, the methodology is bibliographic and documentary, of a legal-dogmatic nature, with a qualitative approach and the use of deductive reasoning, starting from constitutional premises concerning limits on state power and fundamental rights in order to derive criteria applicable to monitoring policies and database integration. Furthermore, a priority temporal scope between 2015 and 2025 is adopted, with the inclusion of indispensable formative works, and a review conducted in repositories

such as SciELO, RedALyC, HeinOnline, SSRN, and Google Scholar. In terms of discussion, the text delineates legal categories such as privacy, intimacy, secrecy, and informational self-determination; examines risks of profiling and selectivity in data ecosystems; and organizes a standard of constitutional control based on strict legality, proportionality, minimization and retention, reservation of jurisdiction where applicable, transparency compatible with security, and mechanisms of auditability and contestation, while also engaging with normative and institutional frameworks in Brazil and Argentina.

Keywords: Constitutional Law; Informational Self-Determination; Informational Surveillance; Interoperability.

1. CONSIDERAÇÕES INICIAIS

A vigilância estatal, por muito tempo, atuou sob a lógica do registro localizado, do documento físico e do acesso limitado por barreiras materiais, em que o prontuário, a ficha, o relatório, a pasta que circulava lentamente entre repartições e, em regra, exigia uma decisão administrativa expressa para ser consultada. Tal arranjo, próprio da vigilância analógica já organizava assimetrias, distribuía suspeitas e desenhava fronteiras entre o normal e o desviante, segundo critérios institucionais que, não raro, se impunham como técnica de governo da vida social, na chave disciplinar descrita por Foucault (1975).

O que se altera, com a digitalização e a datificação das rotinas estatais, é menos a existência do impulso de observar e mais o seu modo de funcionamento, considerando que a vigilância informacional muda o centro de gravidade do ato isolado de coleta para a capacidade contínua de relacionar rastros, inferir padrões e estabilizar identidades por meio de sinais dispersos, redefinindo o que é saber sobre alguém e, dessa maneira, o que é poder sobre alguém. Nessa passagem, a privacidade se projeta como esfera de autodeterminação frente ao olhar institucional, tal como formulado no debate clássico do direito à privacidade informacional por Westin (1967).

A vigilância, nesse panorama, passa a se expressar por perfis e scores, por listas de interesse e por mapas de risco, gerados a partir de integrações que transformam dados originalmente dispersos em uma narrativa unitária sobre a pessoa, com forte vocação de permanência. Do ponto de vista social, essa engenharia não recai uniformemente sobre todos, pois ela opera por seleção, incide com maior intensidade em territórios marcados por precariedade e tende a reiterar classificações históricas de suspeição, na medida em que a própria produção estatal de dados espelha prioridades, práticas e vieses de atuação, como aponta a literatura sociológica sobre vigilância e ordenação social em ambientes digitais (Lyon, 2007).

É nesse ponto que a proteção de dados se mostra como linguagem jurídica apta a rearticular liberdades clássicas em face de tecnologias de observação. Ao se voltar para finalidade, limites e garantias do tratamento, ela modifica o debate do segredo para a legitimidade do processamento e para a distribuição do poder informacional, em linha com a tradição europeia de direitos ligada à pessoa e à sua governança sobre informações que a identificam (Rodotà, 2012).

Esse cenário impõe um problema que, no recorte deste artigo, é ao mesmo tempo constitucional e institucional, que é o fato até que ponto o Estado pode coletar, cruzar e tratar dados pessoais no contexto de políticas de monitoramento e de bancos de dados voltados à segurança pública sem comprometer garantias constitucionais, principalmente quando a própria arquitetura técnica favorece expansão silenciosa de escopos e reuso contínuo de informações por órgãos diversos.

Esse controle se torna ainda mais sensível quando a atuação policial e os sistemas de inteligência se valem de integrações e análises preditivas, pois a vigilância por dados tende a converter históricos de atuação e registros institucionais em aparente evidência objetiva, com efeitos de retroalimentação e perpetuação de assimetrias, como se observa no estudo sobre incorporação de *analytics* em práticas policiais (Brayne, 2017).

Quando dados de origem já comprometida por práticas ilícitas ou discriminatórias passam a treinar e orientar modelos de alocação de recursos e definição de alvos, o risco constitucional se projeta como reprodução ampliada de violações e como reforço institucional de seletividades, conforme advertido no debate sobre *dirty data* e suas consequências na justiça criminal (Richardson; Schultz; Crawford, 2019).

Diante de tal problema, o objetivo deste artigo é identificar parâmetros constitucionais e dogmáticos capazes de orientar o controle das práticas estatais de vigilância baseadas em dados no campo da segurança pública, compreendendo a proteção de dados como limite material à expansão do monitoramento e ao acúmulo indefinido de informações pessoais.

Para tanto, a pesquisa é bibliográfica e documental, de natureza jurídico-dogmática, com abordagem qualitativa e orientação descritivo-analítica, voltada a reconstruir argumentos normativos e a aferir sua aptidão para controlar práticas estatais contemporâneas. Outrossim, adota-se o método de abordagem dedutivo porque o núcleo do problema exige partir de premissas constitucionais e dogmáticas sobre limites ao poder, direitos e garantias, para então extrair critérios aplicáveis a políticas de monitoramento e a bancos de dados, permitindo avaliar se, e em que condições, determinadas práticas podem ser consideradas legítimas.

Os procedimentos metodológicos incluem recorte temporal voltado prioritariamente a produções publicadas entre 2015 e 2025, sem prejuízo de obras formadoras indispensáveis para o enquadramento conceitual, e critérios de inclusão centrados em trabalhos que enfrentem diretamente vigilância estatal por dados no âmbito da segurança pública, governança de bancos estatais, seletividade e impactos distributivos, enquanto se excluem materiais que tratem de decisões automatizadas, de democracia algorítmica ou de aplicações privadas sem pertinência institucional ao problema.

Para a revisão bibliográfica e o mapeamento da produção científica, utilizam-se bases e repositórios que favorecem acesso a literatura jurídica e sociojurídica latino-americana e internacional, em especial SciELO, RedALyC, HeinOnline, SSRN e Google Scholar, escolhidos pela capilaridade temática, pela presença de periódicos importantes nas áreas jurídica e social e pela possibilidade de rastrear debates contemporâneos com estabilidade de metadados.

2. EVOLUÇÃO HISTÓRICA E BASES CONCEITUAIS DO PODER DE VIGILÂNCIA E DA PROTEÇÃO DE DADOS

A história da vigilância estatal, quando observada pelo prisma do Estado moderno, mostra uma mudança de ênfase que reordena as bases anteriores. A vigilância analógica, associada à presença física, ao controle territorial e à inspeção direta, caminhou lado a lado com um processo menos visível e mais persistente, a construção burocrática de identidades documentais.

A identificação civil, os registros, os censos, os prontuários administrativos e policiais e a própria cultura do dossiê foram formando um modo de governar que se apoiava na escrita, na classificação e na recuperação de informações, convertendo pessoas em entradas manejáveis em arquivos. Nesse cenário, a racionalidade administrativa era um vetor de poder, na medida em que o exercício do domínio legal racional dependia de rotinas, competências e registros que garantam previsibilidade, continuidade e imputação de responsabilidades, como já se percebe no retrato da burocracia moderna em Weber (1999).

Ao mesmo tempo, a disciplina, entendida como tecnologia de condução de corpos e condutas, também atuava por formas de observação, anotação e comparação que fazem do registro uma peça do próprio mecanismo de normalização, tal como descrito por Foucault (1987). De tal maneira, antes mesmo da digitalização, já se desenhava uma vigilância informacional, na qual o controle passou a depender do documento que fixa, do formulário que categoriza e do arquivo que permite reconstruir trajetórias.

Quando o horizonte técnico muda para o ambiente informacional, o dado ocupa o lugar que antes era reservado ao papel arquivado, e essa transição altera o alcance e a velocidade do poder de vigilância. O ponto de partida conceitual, no direito brasileiro contemporâneo, é a definição normativa de dado pessoal como informação relacionada a pessoa natural identificada ou identificável, o que demonstra que a proteção recai sobre qualquer informação que, em contexto, permita individualizar alguém, conforme a Lei n. 13.709 (Brasil, 2018).

A mesma lei distingue o dado pessoal sensível, ao associá-lo a esferas informacionais que, por sua natureza, ampliam o risco de discriminação e de exposição indevida, enfatizando que as

categorias jurídicas carregam juízos sobre danos prováveis e exigências reforçadas de justificação (Brasil, 2018).

A noção de identificabilidade, por sua vez, convida a abandonar uma visão estreita, baseada apenas em identificadores diretos, pois o dado identificável pode surgir do encadeamento de fragmentos aparentemente neutros, incluindo metadados. Estes, mesmo quando não mostram conteúdo comunicacional, descrevem padrões de tempo, local, rede, dispositivo e relações, permitindo inferências sobre hábitos, vínculos e rotinas, o que recoloca a discussão sobre proteção em bases contextuais, como observa a doutrina de Doneta (2006) dedicada à passagem da privacidade para a lógica específica da proteção de dados.

É nesse ponto que se torna pertinente destacar a finalidade e o contexto como chaves hermenêuticas, porque a natureza de um dado, seu potencial lesivo e o regime de legitimidade do tratamento variam conforme a operação realizada, o agente que trata e o propósito declarado, e não apenas conforme uma suposta essência da informação.

Essa mudança conceitual exige distinguir, com cuidado dogmático, categorias que muitas vezes são usadas como sinônimos no debate público, contudo, produzem efeitos jurídicos distintos no controle do Estado.

Para Silva (2021), a privacidade, em sentido amplo, costuma designar a esfera de não exposição e de reserva diante de intrusões indevidas, funcionando como parâmetro de limitação do poder público e, em certos casos, como dever de proteção diante de terceiros. Já a intimidade remete a um núcleo mais restrito, ligado à vida interior, a vínculos afetivos e a dimensões existenciais cuja publicização tende a produzir danos mais intensos e duradouros, razão pela qual sua tutela costuma exigir um nível mais elevado de justificativa quando submetida a restrições. O sigilo, por outro espectro, descreve uma técnica jurídica de proteção de fluxos informacionais e comunicacionais, impondo barreiras ao acesso e ao compartilhamento, como se percebe na proteção constitucional do sigilo das comunicações e de dados, que se conecta a garantias processuais e a limites de investigação.

Já a autodeterminação informativa introduz uma mudança de linguagem e de estrutura, pois não se resume a impedir o acesso, visto que a organizar o poder de decidir sobre coleta, uso, circulação e permanência de informações pessoais, sob critérios de legalidade, necessidade e controle institucional, perspectiva que se consolidou na tradição europeia e encontrou formulação influente na obra de Rodotà (2008).

No constitucionalismo contemporâneo, essa categoria tende a agir como eixo de reequilíbrio entre Estado e indivíduo em ambientes de tratamento massivo, já que obriga a administração a justificar finalidades, demonstrar adequação e limitar excessos, trazendo para o centro o problema

das restrições a direitos fundamentais como colisões que exigem ponderação e fundamentação, em linha com a teoria dos princípios elaborada por Alexy (2008).

No caso brasileiro, a incorporação expressa do direito à proteção de dados pessoais no rol de direitos e garantias fundamentais está em consonância com essa autonomização e produz efeitos imediatos na sindicabilidade de políticas públicas de vigilância e de compartilhamento de bases, ao explicitar a densidade constitucional do tema (Brasil, 2022).

No plano sociológico, o debate sobre segurança pública e vigilância ganha inteligibilidade quando lido como forma de governo que administra riscos, antecipa perigos e organiza populações por critérios de suspeição e elegibilidade. A análise de Foucault (2008) sobre segurança e governamentalidade mostra como, ao lado da disciplina, existe uma racionalidade que opera por dispositivos voltados à gestão de circulações, probabilidades e ameaças, especialmente no que se refere os padrões e regularidades.

Tal lógica, ao ser inserida em políticas de monitoramento, tende a produzir uma suspeição difusa, em que a vigilância funciona como triagem permanente, sustentada por dados e por modelos de classificação. Nesse ponto, a crítica de Bigo (2002) à governamentalidade da inquietação é uma questão importante para compreender como o discurso de segurança muda fronteiras entre normalidade e perigo, autorizando práticas rotineiras de verificação, filtragem e perfilização, muitas vezes justificadas por uma gramática de urgência.

A vigilância, então, compõe um arranjo institucional que produz perfis, distribui oportunidades e impõe ônus, selecionando quem circula sem fricção e quem passa a existir sob regimes mais densos de controle.

A citada dimensão seletiva se conecta com a ideia de *panoptic sort*, na qual a economia política da informação organiza a classificação de pessoas segundo valor presumido e risco atribuído, mostrando que a vigilância é também uma tecnologia de diferenciação social (Gandy, 1993). Tal transição sugere que a vigilância contemporânea opera como redes múltiplas, conectadas e heterogêneas, capazes de recombinar sinais e produzir duplos de dados, como descrevem Haggerty e Ericson (2000).

É aqui que se completa o arrasto do arquivo ao banco de dados, com impactos sobre a dogmática constitucional. O arquivo clássico, ainda que volumoso e intrusivo, era marcado por certa inércia material, por custos de manutenção e por limites de circulação, o que funcionava, na prática, como barreira parcial à expansão ilimitada.

O banco de dados, ao contrário, viabiliza interoperabilidade, cruzamentos em larga escala e reuso continuado, com capacidade de transformar finalidades originais em pretextos para novas finalidades, especialmente quando diferentes órgãos e entes compartilham estruturas e chaves de

identificação. Sobre isso, Lyon (2001) descreve esse cenário como transição para uma sociedade em que o monitoramento se naturaliza no cotidiano e se associa a promessas de eficiência, conveniência e proteção, fenômeno que o referido autor examina ao tratar da vigilância como traço ordinário da vida social contemporânea.

No plano da teoria social, o diagnóstico de Deleuze (1992) sobre sociedades de controle antecipa esse ponto ao sugerir que a modulação contínua substitui o confinamento clássico, com controles distribuídos que se exercem por senhas, acessos, créditos e autorizações, sempre dependentes de informação circulante. Igualmente, a descrição de Zuboff (2019) sobre a captura de dados e a produção de previsões comportamentais deixa explícito que o tratamento massivo interessa à polícia ou ao Estado administrativo e também a circuitos econômicos que alimentam mercados de previsão e de indução de condutas, produzindo pressões estruturais por coleta contínua.

Do ponto de vista constitucional, os riscos acompanham esse salto tecnológico e institucional, pois a interoperabilidade e cruzamentos massivos ampliam o risco de erros e de estigmas duradouros, porque uma informação equivocada pode se propagar por vários sistemas e gerar efeitos cumulativos sobre direitos, especialmente quando o indivíduo não tem meios claros de acesso, correção e contestação.

Também, o tratamento em larga escala favorece inferências e classificações que podem afetar igualdade, liberdade de circulação e presunção de inocência, ao transformar correlações em suspeitas e suspeitas em restrições. Em um Estado de Direito, o ponto principal não é negar a legitimidade de políticas de segurança, mas impor a elas deveres de justificação, limites de necessidade e controles institucionais compatíveis com direitos fundamentais, agora expressamente reconhecidos no plano constitucional brasileiro quanto à proteção de dados (Brasil, 2022).

A resposta jurídica exige, nesse cerne, reintroduzir densidade normativa onde a técnica tende a apresentar seus resultados como neutros, e isso passa por exigir finalidade determinada, minimização e transparência compatível com o regime democrático, tal como se extrai dos fundamentos e das definições estruturantes da LGPD (Brasil, 2018).

Nessa perspectiva, o próprio Supremo Tribunal Federal, ao suspender o compartilhamento amplo de dados de usuários de telecomunicações com o IBGE previsto na Medida Provisória 954, enfrentou o problema da insuficiência de garantias e da necessidade de proteção da intimidade e da vida privada em operações de grande escala, deixando claro a centralidade do controle constitucional sobre políticas informacionais do Estado (Brasil, 2020).

Nesse quadro, o poder de vigilância hoje em dia é uma questão de arquitetura institucional da informação, na qual bancos de dados, padrões de interoperabilidade e rotinas de cruzamento se convertem em temas de legalidade, direitos fundamentais e limites democráticos.

3. A PROTEÇÃO DE DADOS COMO LIMITE MATERIAL AO PODER DE VIGILÂNCIA

A tutela informacional, quando compreendida como garantia constitucional, é um limite material ao poder de vigilância porque conduz a discussão do terreno da conveniência administrativa para o da juridicidade, no qual o Estado só pode agir nos termos previamente conformados pelo direito.

Em matéria de restrição a direitos fundamentais, isso exige legalidade estrita e reserva de lei capaz de definir com nitidez hipóteses de atuação, finalidades, sujeitos alcançados, grau de intrusão e salvaguardas, evitando mandatos vagos que permitem expansão contínua de práticas de monitoramento. Nessa moldura, a motivação integra o próprio limite, pois a autoridade deve explicitar por que a medida é admitida, qual o objetivo constitucionalmente legítimo que a sustenta e quais serão seus contornos operacionais, de modo a viabilizar controle e contestação (Canotilho, 2003).

A vinculação de juridicidade, porém, não se esgota na lei e na motivação, porque a vigilância por dados tende a transformar decisões para rotinas administrativas e sistemas técnicos pouco visíveis. Por isso, o limite material precisa incorporar deveres de controle e responsabilidade estatal, com trilhas de auditoria, registros de acesso, governança de compartilhamento e mecanismos de apuração de desvios e abusos, inclusive quando o dano decorre de falhas de segurança ou de tratamento inadequado. Nessa perspectiva, a proteção de dados é uma cláusula de contenção da opacidade, tornando indevida a ideia de que a dificuldade técnica do controle serve como justificativa para reduzir a exigência de prestação de contas (Sarlet, 2012).

No que lhe concerne, a proporcionalidade é o método mais produtivo para converter essas exigências em critérios verificáveis, especialmente em vigilância orientada por bases estatais e monitoramento contínuo. A adequação, aqui, não se satisfaz com a afirmação genérica de que coletar ajuda, pois requer demonstração mínima de aptidão real para o fim declarado, distinguindo políticas baseadas em evidência de estratégias baseadas em intuição institucional. Quando a triagem depende de perfis e correlações, o Estado deve explicar quais relações de causalidade ou de risco justificam o tratamento, sob pena de apoiar-se em generalizações que ampliam o poder de observação sem lastro racional (Alexy, 2008).

A necessidade, no campo dos dados, impõe um exame mais rígido do que costuma aparecer em práticas administrativas, porque alternativas menos intrusivas existem e frequentemente são mais compatíveis com a Constituição.

Ou seja, medidas pontuais e temporárias, anonimização efetiva, segmentação de acesso, coleta sob demanda e políticas de segurança da informação podem reduzir o impacto sobre a vida privada sem inviabilizar fins públicos legítimos. Esse ponto é necessário no setor público, pois a capacidade de integrar bases e replicar acessos torna tentadora a expansão por conveniência, e o teste de necessidade serve para impedir que o Estado escolha sempre o caminho mais invasivo por ser tecnicamente mais fácil (Doneda, 2006).

A proporcionalidade em sentido estrito, por sua vez, exige que se leve a sério o saldo de perdas e ganhos constitucionais, e não apenas o benefício alegado em abstrato. Isto é, bases extensas elevam o risco de vazamentos e de reutilizações indevidas, produzem efeitos inibitórios sobre a vida cotidiana e aumentam assimetrias de poder informacional entre Estado e indivíduo. O ponto não é negar políticas públicas de segurança, mas obrigá-las a demonstrar que o custo imposto ao conjunto dos direitos não supera o benefício obtido, maiormente quando a vigilância se aproxima de lógicas permanentes de observação e classificação (Rodotà, 2008).

Esses testes se conectam diretamente aos princípios de finalidade, minimização e retenção, que são barreiras constitucionais à cultura de coletar primeiro e justificar depois. A finalidade precisa ser específica e delimitada, sem autorização para ampliação oportunista de escopo, e a minimização deve orientar o desenho institucional e a arquitetura técnica, reduzindo campos, granularidade e frequência de coleta ao estritamente necessário. Já a retenção demanda prazos e rotinas de eliminação compatíveis com a finalidade declarada, porque a guarda indefinida transforma estoques de dados em promessa permanente de novos usos, com efeitos cumulativos sobre a privacidade e sobre a liberdade de circulação social (Brasil, 2018).

A disciplina jurídica brasileira abona, inclusive, instrumentos normativos que ajudam a densificar esses critérios no âmbito do Estado. A Lei Geral de Proteção de Dados, ao estruturar princípios como finalidade, adequação e necessidade, e ao prever direitos do titular, dá linguagem normativa para exigir que políticas de dados sejam justificadas antes e durante sua execução, com transparência, segurança e governança de acesso. Nessa mesma direção, o Marco Civil da Internet traz que registros e acessos devem ser disciplinados por regras compatíveis com direitos fundamentais, o que impede que o Estado trate a infraestrutura informacional como espaço de livre exploração por razões de utilidade administrativa (Brasil, 2014).

Quando a vigilância alcança dados cobertos por sigilo constitucional ou quando a intrusão é elevada, a reserva de jurisdição opera como salvaguarda que aumenta o limite material. O acesso a conteúdos e a determinadas categorias sensíveis de dados não pode ser naturalizado como rotina administrativa, exigindo autorização judicial com fundamentação individualizada, delimitação temporal e precisão de objeto, sob pena de converter exceções em normalidade. O fato de nem todo

tratamento depender de juiz não autoriza expansão por ato infralegal, pois a própria Constituição condiciona intervenções mais invasivas a formas rígidas de controle, e a ausência dessas formas compromete a legitimidade da medida (Brasil, 1988).

Mesmo quando a autorização judicial não é exigida, medidas intrusivas precisam ser acompanhadas por salvaguardas que impeçam desvio de finalidade e abuso de acesso, assim, envolvendo a delimitação do escopo, segregação de perfis de usuário, logs auditáveis, cadeia de custódia e mecanismos independentes de revisão, capazes de reconstruir o caminho do dado desde a coleta até o uso final. A técnica torna o acesso silencioso mais fácil, e é justamente por isso que o direito deve impor fricções institucionais que preservem o controle democrático sobre práticas de vigilância, recusando a transformação da opacidade em regra (Bioni, 2019).

O limite material também se realiza como defesa informacional, pois o indivíduo não pode ser reduzido a objeto de classificação estatal sem instrumentos reais de contestação. Para tanto, direito de acesso a registros, conhecimento sobre finalidades e compartilhamentos, correção de dados inexatos e possibilidade de impugnação são exigências que aproximam a proteção de dados do devido processo em ambiente informacional.

A partir de tal visão, quando decisões estatais são influenciadas por tratamento automatizado, a exigência de explicação deve produzir razões compreensíveis e contestáveis, com vias administrativas e judiciais aptas a reverter efeitos indevidos, evitando que probabilidades estatísticas se tornem rótulos estáveis sem contraditório (Doneda, 2006).

A sociologia do controle ajuda a visualizar por que esses direitos de defesa não são mero detalhe procedimental. A vigilância contemporânea age por triagens e ordenações que distribuem acesso e restrições, fazendo com que dados sejam critérios de filtragem social, muitas vezes com efeitos discriminatórios indiretos. O *panoptic sort*, citado anteriormente, descreve esse processo de classificação como forma de gestão de riscos e oportunidades, no qual o tratamento de informações produz hierarquias e inclui ou exclui sujeitos de circuitos sociais e institucionais, mesmo sem que isso seja explicitado como política pública (Gandy, 1993).

A expansão de bases e cruzamentos também se articula ao que a doutrina descreve como *assemblage* de vigilância, na qual diferentes sistemas e instituições são conectados, produzindo um campo ampliado de observação e rastreamento. Nesse ambiente, o dado circula com rapidez, perde contexto e ganha novas finalidades por acoplamento institucional, e isso eleva o risco de que práticas de segurança se tornem mecanismos difusos de governo da vida cotidiana. A contenção constitucional, como consequência, precisa mirar a circulação e a integração, e não apenas o momento inicial da coleta, pois é na recombinação que muitos impactos se tornam duradouros (Haggerty; Ericson, 2000).

A dimensão social do limite material fica ainda mais notória quando se observam estigmatização, seletividade penal e territorialização da vigilância. Em contextos marcados por desigualdade, a observação tende a se concentrar em territórios pobres e em populações já vulnerabilizadas, aumentando a produção institucional de suspeitas e a naturalização de abordagens seletivas.

Na chave latino-americana, a crítica à seletividade do sistema penal mostra como práticas de controle costumam operar sobre alvos preferenciais, e a vigilância por dados pode ampliar essa seletividade ao automatizar triagens e ao tornar permanentes registros que acompanham sujeitos e territórios ao longo do tempo (Zaffaroni, 1991).

Também há risco quando o vocabulário de segurança se combina com lógicas de exceção e com regimes de suspeita que capturam o dissenso e a mobilização política, considerando que a securitização pode modificar direitos como problemas, transformando protesto em risco e organização social em indicador, de maneira especial quando o Estado utiliza bancos e cruzamentos para mapear redes, deslocamentos e associações. A crítica contemporânea da vigilância mostra que o poder informacional pode se expandir por camadas, com justificativas sucessivas e baixa transparência pública, e esse movimento exige que a proteção de dados seja lida como garantia contra a normalização de medidas extraordinárias no cotidiano (Bigo, 2006).

A economia política da vigilância também é importante para compreender por que o limite material precisa ser bem desenvolvido no setor público, ainda que a discussão costume se concentrar em empresas. A consolidação de infraestruturas de rastreamento, perfis e previsões cria incentivos institucionais para ampliar coleta e integração, porque o estoque de dados passa a ser visto como ativo estratégico, e a autoridade pública tende a justificar novos usos pela simples disponibilidade do acervo.

Nessa toada, a crítica ao capitalismo de vigilância, embora dirigida ao setor privado, ajuda a compreender como a captura e a exploração de dados podem reorganizar relações de poder e reduzir espaços de autonomia, com efeitos sobre liberdade e igualdade que não podem ser tratados como externalidades aceitáveis (Zuboff, 2019).

Nesse quadro, a proteção de dados como limite material ao poder de vigilância se afirma como exigência dogmática que conecta legalidade estrita, proporcionalidade, finalidades definidas, minimização e retenção, reserva de jurisdição quando necessária, salvaguardas técnicas e institucionais e direitos de defesa informacional.

Ao mesmo tempo, ela precisa reconhecer que vigilância é prática social que distribui visibilidade e invisibilidade, e que, sem contenção, tende a aumentar hierarquias, estigmas e controles sobre pobreza e dissenso. A racionalidade constitucional do limite, de tal modo, se orienta por uma

ideia de cidadania que recusa a governança por suspeitas permanentes, exigindo que o Estado prove, antes de vigiar, que pode fazê-lo dentro das formas e das razões admitidas pelo direito.

4. CONTROLE CONSTITUCIONAL E ARRANJOS INSTITUCIONAIS NO BRASIL E NA ARGENTINA

A partir da discussão apresentada, nessa parte final do trabalho, o ponto mais importante para compreender políticas estatais de monitoramento baseadas em dados, em ambos os países, é reconhecer que elas se instalam em arquiteturas normativas que combinam cláusulas constitucionais de direitos e garantias e, bem como, arranjos institucionais que distribuem competências entre segurança pública, inteligência, administração e controle.

No caso brasileiro, a Constituição de 1988 preserva um modelo de direitos fundamentais e, ao mesmo tempo, organiza a segurança pública como dever do Estado e responsabilidade compartilhada em um campo federativo marcado por assimetrias administrativas e informacionais, com reflexos sobre a produção e o uso de bancos de dados oficiais (Brasil, 1988).

Esse enquadramento se adensa com a Lei Geral de Proteção de Dados Pessoais, que estabelece princípios e bases legais para o tratamento de dados inclusive pelo poder público, sem dispensar o vínculo estrito entre finalidade, necessidade e adequação, e com marcos setoriais como o Sistema Único de Segurança Pública, que pretende ordenar diretrizes, integração e governança em um setor historicamente fragmentado (Brasil, 2018a).

Na Argentina, a reforma constitucional de 1994 conferiu estatuto explícito ao habeas data e consolidou uma porta constitucional para a disputa sobre arquivos, registros e bancos de dados, ao lado das demais garantias do devido processo e da liberdade pessoal, o que produz um vocabulário próprio para enfrentar abusos de classificação e vigilância por informação (Argentina, 1994).

Ainda, a Ley 25.326 fixou um regime geral de proteção de dados com direitos do titular e regras para bancos de dados públicos e privados, enquanto os regimes vinculados à segurança interior e à inteligência nacional estruturam competências e autorizam práticas que, em contextos de ameaça, tendem a tensionar o patamar ordinário de proteção de direitos, exigindo filtros institucionais ainda mais nítidos para evitar normalização de exceções (Argentina, 2000).

Quando se passa do plano normativo ao plano dos bancos de dados estatais e da integração informacional, a discussão é sobre desenho administrativo e garantias técnicas que tornam verificável a legalidade do acesso e do uso. A sociologia do controle ajuda a nomear essa questão, porque práticas de vigilância raramente operam como um ato único e visível, mas como ecossistemas de coleta,

correlação e circulação que tornam sujeitos legíveis por meio de classificações, perfis e antecipações de risco, com efeitos distribuídos na vida social (Foucault, 1987).

Essa leitura se cruza com a crítica da *dataveillance* e da triagem informacional, que mostra como bases integradas podem ordenar oportunidades e suspeitas por critérios que incidem sobre grupos e territórios de maneira desigual (Gandy Jr., 1993).

É nesse ponto que critérios de criação e governança dos bancos de dados públicos se tornam, eles próprios, matéria de controle constitucional, porque a legalidade de um programa não se esgota na existência formal de um banco, pois ela depende de justificativa pública para sua finalidade, de definição de categorias de dados e prazos, de regras de qualidade, atualização e retificação, e de uma cadeia de responsabilidade por acessos e compartilhamentos.

No Brasil, a LGPD fornece um eixo de princípios e deveres para o setor público, e o Decreto 10.046, ao tratar de governança de compartilhamento de dados na administração pública federal e instituir o Cadastro Base do Cidadão, explicita a centralidade de interoperabilidade, padronização e instâncias de governança, o que recoloca o debate sobre integração sob uma chave de rastreabilidade e *accountability*, e não como simples eficiência administrativa (Brasil, 2019).

Em termos de controle, esse tipo de arranjo só se sustenta democraticamente quando a interoperabilidade vem acompanhada de trilhas de auditoria, registros de acesso e capacidade de reconstrução posterior de quem consultou o quê, quando, com qual fundamento e para qual finalidade, pois é essa reconstrução que converte o princípio em prova.

Na Argentina, a experiência de sistemas de identificação e bases orientadas à segurança, como o SIBIOS, mostra como a integração pode ganhar densidade biométrica e, por isso, ampliar riscos de usos desviados e de efeitos discriminatórios caso a governança não seja desenvolvida por controles internos e externos capazes de enfrentar a opacidade técnica e o argumento recorrente de sigilo (Argentina, 2011).

Mesmo quando a base é instituída por norma válida, o problema constitucional reaparece na vida cotidiana do sistema, porque é no acesso reiterado e na correlação entre bancos que se forma o duplo informacional do indivíduo, descrito pela literatura de *assemblage*, com potencial de recodificar pessoas em fluxos de dados que circulam por finalidades diversas (Haggerty; Ericson, 2000).

Diante disso, modelos de controle precisam ser criados como uma ecologia institucional que combina controle judicial, administrativo e político-institucional em camadas, para reduzir incentivos ao abuso e aumentar a probabilidade de detecção.

No constitucionalismo brasileiro, a tradição de controle de constitucionalidade, com convivência entre controle concentrado e difuso, apresenta um sistema apto para ponderar restrições

a direitos e exigir justificações públicas, inclusive quando o Estado invoca segurança para reduzir transparência, e é nessa gramática que se inserem exigências de proporcionalidade, necessidade e adequação em medidas de tratamento massivo de dados (Mendes; Branco, 2021).

A teoria dos limites a direitos, com sua estrutura de princípios e regras de justificativa, é um método para evitar que a cláusula de segurança opere como permissão genérica, tranasformando o debate para critérios verificáveis e revisáveis (Alexy, 2008).

No plano administrativo e político-institucional brasileiro, a presença do Ministério Público, das defensorias, dos tribunais de contas e da autoridade de proteção de dados cria um circuito potencialmente virtuoso, desde que cada órgão atue dentro de suas competências e com coordenação mínima. O Ministério Público tem vocação para tutela de direitos coletivos e fiscalização de políticas públicas, o que o habilita a questionar programas de monitoramento quando faltam base legal, delimitação de finalidade e medidas de mitigação de risco.

As defensorias, por sua vez, são canais privilegiados para transformar opacidades em litigância estratégica e para dar forma procedimental à contestação por pessoas afetadas, especialmente quando o impacto da classificação recai sobre grupos vulneráveis. Bem como, Tribunais de contas podem incorporar auditorias de governança de dados e de integridade de acessos como parte do exame de economicidade e conformidade, e a autoridade nacional de proteção de dados, criada pela alteração legislativa da LGPD, possui função de orientação regulatória, fiscalização e sanção administrativa, colaborando para que o controle não dependa exclusivamente do Judiciário (Brasil, 2019a).

Na Argentina, a tradição do controle judicial difuso e a centralidade da Corte Suprema na estabilização interpretativa convivem com uma cultura constitucional em que ações como o amparo e o habeas data têm papel importante na tutela de direitos frente a bancos de dados, justamente porque permitem discutir o acesso, a retificação e a finalidade do tratamento em chave de garantia.

A doutrina constitucional argentina, ao tratar de desenho institucional e de tensões entre poderes, entendem que garantias se realizam por mecanismos concretos de contestação e revisão, o que é sensível em matéria de segurança e inteligência, onde a assimetria informacional favorece o Estado (Sagüés, 2017).

Ao lado disso, a autoridade de aplicação em matéria de dados e acesso à informação, no âmbito estatal, pode funcionar como instância técnica de controle e de mediação, desde que tenha independência prática e capacidade de impor correções em políticas e bases (Argentina, 2016).

As garantias procedimentais em políticas de monitoramento são o ponto em que a dogmática constitucional encontra a engenharia de governança, exigindo transparência compatível com a proteção de operações, o que significa, ao menos, tornar públicos os objetivos do programa, as

categorias de dados tratadas, as bases legais utilizadas, as métricas agregadas de acesso, os critérios gerais de compartilhamento e os relatórios de impacto e conformidade.

A Lei de Acesso à Informação, no Brasil, apresenta uma moldura para esse equilíbrio ao afirmar o direito de acesso e, ao mesmo tempo, admitir hipóteses de restrição que devem ser motivadas e temporárias, evitando a naturalização do sigilo como padrão (Brasil, 2011). Em um programa de monitoramento por dados, a finalidade precisa ser delimitada de modo operativo, porque, sem isso, a integração informacional tende a se transformar em repositório multiuso, e a experiência comparada mostra que repositórios multiuso são os que mais facilmente abrigam deriva funcional.

A mesma lógica vale para canais de contestação, posto que, não basta reconhecer, em tese, direitos de acesso, correção e eliminação quando cabíveis, sendo necessário construir fluxos acessíveis de requerimento, prazos e respostas, inclusive com possibilidade de revisão por instâncias independentes, para que a contestação não seja apenas simbólica.

Ao lado disso, há deveres de documentação que precisam ser assumidos como condição do próprio programa, e não como formalidade posterior, tendo em vista que sem documentação, não há auditabilidade, e sem auditabilidade o controle se converte em confiança cega, o que é incompatível com políticas que ampliam poder informacional do Estado.

Nessa linha, prevenção de usos desviados depende de desenho, e desenho implica separar perfis de acesso por função, registrar consultas, limitar exportações, impor justificativa para acessos sensíveis, criar alertas de padrões anômalos e prever sanções administrativas e disciplinares efetivas para consultas indevidas.

Em democracias desiguais, esse viés aumenta o dever constitucional de cautela, porque bancos e algoritmos podem recodificar estigmas históricos em padrões supostamente neutros, e é nesse ponto que a dogmática do núcleo essencial de direitos e a exigência de igualdade material se convertem em critérios concretos de revisão institucional (Sarlet, 2024).

5. CONSIDERAÇÕES FINAIS

Finalizando o presente artigo, é possível concluir que a vigilância estatal, quando modificada para a lógica de bancos interoperáveis, perfis e correlações permanentes, é uma infraestrutura capaz de produzir efeitos jurídicos e sociais mesmo sem ordem individualizada, contraditório ou visibilidade pública.

Nessa ótica, a proteção de dados age como critério de validade, exigindo finalidade determinada, necessidade demonstrável, retenção limitada, governança rastreável e fricções

institucionais que impeçam a deriva funcional e a naturalização do acesso silencioso, sob pena de a suspeita se converter em método ordinário de governo.

De tal maneira, onde não houver base legal clara, controles auditáveis e possibilidade real de contestação e correção, a vigilância por dados tende a se afastar do Estado de Direito e a aproximar-se de um regime de classificação contínua, incompatível com a proteção constitucional da vida privada e com a tutela autônoma dos dados pessoais.

Um Estado que coleta sem limites aprende a governar por suposições, bem como um Estado que se limita pelo direito aprende a governar por razões. Dessarte, este artigo objetivou explicar que a legitimidade do monitoramento se mede pela qualidade das justificativas, pela proporcionalidade aplicada com seriedade, pela reserva de jurisdição nas hipóteses de maior intrusão e pela existência de mecanismos de *accountability* capazes de reconstruir quem acessou, por quê, por quanto tempo e com quais salvaguardas.

Quando esse padrão é observado, a proteção de dados se afirma como limite material ao poder de vigilância, preservando a liberdade cotidiana contra a triagem permanente e impedindo que a eficiência informacional substitua o controle democrático.

REFERÊNCIAS

ALEXY, Robert. **Teoria dos direitos fundamentais**. 2. ed. São Paulo: Malheiros, 2008.

ARGENTINA. **Constitución de la Nación Argentina (1994)**. Buenos Aires, 1994. Disponível em: https://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm. Acesso em: 17 jan. 2026.

ARGENTINA. **Decreto n. 1766/2011**. Créase el Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS). Buenos Aires, 2011. Disponível em: https://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/189382/norma.htm. Acesso em: 17 jan. 2026.

ARGENTINA. **Ley n. 24.059**. Seguridad Interior. Buenos Aires, 1992. Disponível em: https://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=458. Acesso em: 17 jan. 2026.

ARGENTINA. **Ley n. 25.326**. Protección de los Datos Personales. Buenos Aires, 2000. Disponível em: https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm. Acesso em: 17 jan. 2026.

ARGENTINA. **Ley n. 25.520**. Ley de Inteligencia Nacional. Buenos Aires, 2001. Disponível em: https://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/texact.htm. Acesso em: 17 jan. 2026.

ARGENTINA. **Ley n. 27.275**. Derecho de Acceso a la Información Pública. Buenos Aires, 2016. Disponível em: https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/norma.htm. Acesso em: 17 jan. 2026.

BARROSO, Luís Roberto. **Curso de direito constitucional contemporâneo**. São Paulo: Saraiva Jur, 2024.

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

BIGO, Didier. Security and immigration: toward a critique of the governmentality of unease. **Alternatives**, v. 27, n. 1 Suppl., p. 63-92, 2002.

BIGO, Didier. **Security, exception, ban and surveillance**. In: LYON, David (ed.). Theorizing surveillance: the panopticon and beyond. Cullompton: Willan Publishing, 2006.

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

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 17 jan. 2026.

BRASIL. **Decreto n. 10.046, de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10046.htm. Acesso em: 17 jan. 2026.

BRASIL. **Emenda Constitucional n. 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 competência privativa da União. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 17 jan. 2026.

BRASIL. **Lei n. 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; altera a Lei n. 8.112, de 11 de dezembro de 1990; revoga a Lei n. 11.111, de 5 de maio de 2005, e dispositivos da Lei n. 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 17 jan. 2026.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 17 jan. 2026.

BRASIL. **Lei n. 13.675, de 11 de junho de 2018**. Institui o Sistema Único de Segurança Pública (Susp) e cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS). Brasília, DF:

Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13675.htm. Acesso em: 17 jan. 2026.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 17 jan. 2026.

BRASIL. **Lei n. 13.853, de 8 de julho de 2019**. Altera a Lei n. 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 17 jan. 2026.

BRASIL. Supremo Tribunal Federal. **STF suspende compartilhamento de dados de usuários de telefônicas com o IBGE**. Notícia. Brasília, DF, 7 maio 2020. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902. Acesso em: 17 jan. 2026.

BRAYNE, Sarah. Big data surveillance: the case of policing. **American Sociological Review**, v. 82, n. 5, p. 977-1008, 2017.

CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da constituição**. 7. ed. Coimbra: Almedina, 2003.

DELEUZE, Gilles. Postscript on the societies of control. **October**, v. 59, p. 3-7, 1992.
DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

FOUCAULT, Michel. **Segurança, território, população**: curso dado no Collège de France (1977-1978). Tradução de Eduardo Brandão. São Paulo: Martins Fontes, 2008.

FOUCAULT, Michel. **Surveiller et punir**: naissance de la prison. Paris: Gallimard, 1975.

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. Tradução de Raquel Ramalhete. Petrópolis: Vozes, 1987.

GANDY JR., Oscar H. **The panoptic sort**: a political economy of personal information. Boulder: Westview Press, 1993.

GARGARELLA, Roberto. **La sala de máquinas de la Constitución**: dos siglos de constitucionalismo en América Latina (1810–2010). Buenos Aires: Katz, 2014.

HAGGERTY, Kevin D.; ERICSON, Richard V. The surveillant assemblage. **The British Journal of Sociology**, v. 51, n. 4, p. 605-622, 2000.

LYON, David. **Surveillance society**: monitoring everyday life. Buckingham; Philadelphia: Open University Press, 2001.

LYON, David. **Surveillance studies**: an overview. Cambridge: Polity, 2007.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. São Paulo: Saraiva Educação, 2021.

RICHARDSON, Rashida; SCHULTZ, Jason M.; CRAWFORD, Kate. Dirty data, bad predictions: how civil rights violations impact police data, predictive policing systems, and justice. **New York University Law Review Online**, v. 94, p. 192-233, 2019.

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

RODOTÀ, Stefano. **Il diritto di avere diritti**. Roma-Bari: Laterza, 2012.

SAGÜÉS, Néstor Pedro. **Derecho constitucional**. Buenos Aires: Astrea, 2017.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. 14. ed. Porto Alegre: Livraria do Advogado, 2024.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 14, n. 42, p. 179-218, 2020.

SILVA, Virgílio Afonso. **Direito constitucional brasileiro**. Universidade de São Paulo, 2021.

WEBER, Max. **Economia e sociedade**: fundamentos da sociologia compreensiva. Tradução de Régis Barbosa e Karen Elsabe Barbosa. Brasília, DF: Editora Universidade de Brasília; São Paulo: Imprensa Oficial do Estado de São Paulo, 1999.

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

ZAFFARONI, Eugenio Raúl. **Em busca das penas perdidas**: a perda da legitimidade do sistema penal. Rio de Janeiro: Revan, 1991.

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