

Do capitalismo de vigilância à vigilância biométrica estatal

o poder informacional e seus limites constitucionais

Murillo Sapia Gutier

Advogado

murillo@gutier.adv.br

28 de agosto de 2026

1

1. **Palavras-chave:** Poder informacional. Capitalismo de vigilância. Excedente comportamental. Poder instrumentário. Autodeterminação informativa. Vigilância biométrica. Reconhecimento facial. Discriminação algorítmica. LGPD. EC nº 115/2022.

1. Introdução: um único fenômeno, duas faces

Imagine-se uma pessoa que sai de casa pela manhã. O celular registra seus deslocamentos, as plataformas registram seus cliques e, ao atravessar a praça central, uma câmera pública compara seu rosto, em tempo real, com bancos de dados policiais. São duas engrenagens de um mesmo fenômeno: o **poder informacional**, que tanto pode ser exercido por corporações privadas quanto pelo próprio Estado. Compreender uma face sem a outra é compreender apenas metade do problema.²

Este artigo correlaciona três blocos de conhecimento. O primeiro é o diagnóstico de **economia política** formulado por Shoshana Zuboff: **a descrição do poder que emerge quando organizações acumulam capacidade extraordinária de conhecer e influenciar comportamentos**. O segundo é a resposta de **direito dogmático** oferecida por Danilo Doneda: a estrutura jurídica necessária para proteger a pessoa quando seus dados se convertem em elemento permanente de decisões e classificações. O terceiro é a transposição desse arcabouço para a **vigilância biométrica estatal**, campo em que a jurisprudência do STF construiu um verdadeiro standard de controle.³

2. O diagnóstico de Zuboff: o capitalismo de vigilância

2.1 O excedente comportamental como matéria-prima

A tese central de Zuboff identifica uma **nova lógica de acumulação econômica**, na qual a própria experiência humana é transformada em matéria-prima informacional. Ao utilizar serviços digitais, o usuário produz os dados estritamente necessários à prestação do serviço — mas gera, ao mesmo tempo, um volume muito superior de informações sobre hábitos, deslocamentos, interesses e padrões de conduta. Esse resíduo, denominado **excedente comportamental** (“*behavioral surplus*”), é apropriado, processado e convertido em **produtos de predição**, comercializados junto a quem deseja antecipar o que as pessoas provavelmente farão.⁴

2.2 A cadeia de valor da predição e sua generalização

A dinâmica pode ser decomposta em quatro etapas encadeadas: a **experiência humana** gera sinais comportamentais; o excedente é extraído de modo contínuo;

2. Cf. Zuboff, 2021; Doneda, 2006.

3. Cf. Zuboff, 2021; Doneda, 2006.

4. Cf. Zuboff, 2021.

modelos computacionais realizam a **previsão do comportamento**; e as previsões convertem-se em **valor econômico** — lucro e influência. O ponto decisivo é que esse modelo, nascido na publicidade digital, generaliza-se: penetra seguros, saúde, automóveis, finanças, educação e dispositivos “inteligentes”. A equação é expansiva por natureza: mais dados produzem melhores correlações, melhores previsões e maior valor extraído.⁵

2.3 Do observar ao modular: o poder instrumentário

Há, na arquitetura do sistema, um **incentivo estrutural** que conduz da observação à intervenção: é mais fácil prever determinada conduta quando se pode influenciá-la. Daí a passagem da mera coleta para formas ativas de modulação — arquitetura de escolha, recomendações, notificações, ordenação de conteúdos e personalização. Nesse contexto, formula-se o conceito de **poder instrumentário** (“instrumentarian power”): modalidade de poder que utiliza infraestruturas digitais para observar, calcular e orientar comportamentos em grande escala. O poder deixa de significar “eu sei o que você fez” e passa a significar “posso modificar o ambiente para aumentar a probabilidade de determinada escolha”.⁶

2.4 O espelho unilateral e a assimetria de poder

A metáfora do **espelho unilateral** ilustra a desigualdade estrutural da relação: a organização vê o usuário, mas o usuário não enxerga o processo pelo qual é observado, classificado e previsto. O indivíduo conhece muito pouco sobre a plataforma e seus algoritmos; a plataforma, em contrapartida, conhece milhares de atributos, correlações e inferências sobre aquele indivíduo e sobre milhões de pessoas semelhantes. A **assimetria informacional** transforma-se, assim, em **assimetria de poder**: algoritmos classificam, inferem capacidade econômica e influenciam oportunidades sem que ser humano algum jamais “leia” as informações.⁷

3. A resposta de Doneda: a proteção de dados como disciplina do poder

3.1 A insuficiência da privacidade-segreto

Se Zuboff descreve a doença, Doneda prescreve o remédio jurídico. Em obra pioneira de 2006, o autor sustenta que a transformação tecnológica exige categoria mais ampla que a privacidade em sua feição tradicional. A **privacidade clássica** concentra-se na esfera reservada e responde à pergunta “essa informação é secreta?”. A

5. Cf. Zuboff, 2021. A cadeia aqui descrita corresponde, na parte 2 deste díptico, à taxonomia da memória algorítmica e ao poder de inferir (itens 8.3 e 8.4).

6. Cf. Zuboff, 2021.

7. Cf. Zuboff, 2021.

proteção de dados, diversamente, disciplina o poder produzido pelo tratamento de informações e responde à pergunta “que tratamento está sendo realizado?”. A consequência é notável: pode haver violação da proteção de dados sem que segredo algum tenha sido revelado.⁸

3.2 Autodeterminação informativa e os limites do consentimento

Proteger dados não é apenas colher consentimentos. A pessoa precisa ocupar uma **posição juridicamente relevante** ao longo de todo o ciclo de tratamento de suas informações — é o núcleo da **autodeterminação informativa**. O argumento ganha força diante de uma constatação sociológica: em sociedades informatizadas, entregar dados tornou-se condição de participação econômica e social; recusar todo tratamento pode significar recusar banco, emprego, saúde e serviços públicos. Por isso, a legislação precisa fixar **limites objetivos ao tratamento**, independentes da vontade individual — ideia estruturante da LGPD.⁹

3.3 As quatro gerações legislativas e a constitucionalização

Doneda sistematiza a evolução normativa em quatro gerações: a primeira controlou grandes bancos de dados computadorizados, sobretudo estatais; a segunda conferiu ao indivíduo poder de reação contra usos indevidos; a terceira consagrou a autodeterminação informativa; a quarta instituiu garantias objetivas, tutela reforçada de **dados sensíveis** e autoridades independentes. O que o autor apresentava, em 2006, como interpretação constitucional converteu-se em jurisprudência — o STF reconheceu a proteção de dados como **direito fundamental autônomo** — e, depois, em texto expresse, com a EC 115/2022 (art. 5º, LXXIX, da CF).¹⁰

4. A transposição do problema para o Estado: a vigilância algorítmica e biométrica

4.1 Conceito e modalidades técnicas

O mesmo aparato descrito por Zuboff no mercado pode ser mobilizado pelo Estado. A **vigilância algorítmica** consiste no emprego de sistemas computacionais para coletar, cruzar, classificar, inferir e prever comportamentos a partir de grandes bases de dados; a conjugação entre inteligência artificial, “big data” e **reconhecimento biométrico** converte corpos anônimos em sujeitos permanentemente identificáveis. Três modalidades se distinguem: a **autenticação (1:1)**, que verifica se a pessoa é

8. Cf. Doneda, 2006.

9. Cf. Doneda, 2006.

10. Cf. Doneda, 2006. A construção doutrinária foi posteriormente juridificada pelo STF nas ADIs 6.387, 6.388, 6.389, 6.390 e 6.393 (MC-Ref., Rel. Min. Rosa Weber, Plenário, j. 07/05/2020) e convertida em texto constitucional expresse pela EC nº 115/2022, que inseriu o inciso LXXIX no art. 5º da Constituição.

quem afirma ser; a **identificação retrospectiva (1:N)**, que compara uma imagem com um banco de imagens; e a **identificação remota em massa (N:N)**, na qual câmeras captam rostos indiscriminadamente — a forma que mais se aproxima de uma sociedade de vigilância.¹¹

4.2 As cinco dimensões do problema

Cinco vetores concentram a preocupação constitucional. A **escalabilidade**: milhões de pessoas tornam-se objetos de identificação automatizada sem qualquer ato suspeito. A **autodeterminação informativa**: a biometria, diferentemente de uma senha, não pode ser “trocada” quando comprometida. A **opacidade algorítmica**: qual algoritmo, qual limiar, qual taxa de falsos positivos, quem audita, como impugnar? A **discriminação algorítmica**: os resultados dependem do banco, das categorias e do contexto social — a tecnologia não é neutra. E a **expansão progressiva da finalidade**: bancos criados para fins limitados expandem-se para segurança pública, investigação e inteligência.¹²

4.3 Discriminação algorítmica e “vigilância negra”

O conceito de “**vigilância negra**” explicita que os algoritmos não são socialmente neutros: inserem-se em estruturas históricas de disciplinamento de corpos negros. A desigualdade pode se instalar antes de qualquer erro do sistema — na concentração territorial das câmeras, na composição dos bancos de imagens e nas prioridades das listas de busca. Três espécies se distinguem: o **erro diferencial** (a tecnologia performa desigualmente entre grupos demográficos), a **seleção diferencial** (certos grupos são submetidos à tecnologia com maior frequência) e o **efeito diferencial** (a identificação desencadeia consequências desproporcionalmente graves para grupos específicos, por força de práticas institucionais preexistentes).¹³

Aqui a correlação com Zuboff é direta: o espelho unilateral privado reaparece, agravado, na relação entre Estado e cidadão. E a correlação com Doneda é igualmente evidente: a impossibilidade de “trocar” a biometria e a opacidade dos sistemas demonstram que o consentimento individual é resposta insuficiente, exigindo-se limites objetivos, auditáveis e contestáveis ao tratamento estatal.¹⁴

11. As seções 4 a 6 sistematizam os slides do autor sobre a vigilância algorítmica e biométrica pelo Estado. As correlações com Zuboff, 2021, e Doneda, 2006, são construções do presente texto.

12. Cf. art. 5º, LXXIX, da Constituição, incluído pela EC nº 115/2022; Doneda, 2006. A escalabilidade corresponde, na parte 2 deste díptico, à mutação informacional pela escala (item 8.1): trata-se do mesmo fenômeno, observado nos eixos do presente e do tempo.

13. Ver nota 10.

14. Cf. Zuboff, 2021; Doneda, 2006.

5. O standard do STF: quatro camadas de controle do poder informacional estatal

5.1 Controle informacional

A primeira camada nasceu no caso IBGE. Nas **ADIs 6.387 e conexas**, o STF suspendeu a MP 954/2020, que impunha o compartilhamento de dados de usuários de telefonia com o IBGE, e firmou a mudança de paradigma: o exame constitucional considera, conjuntamente, o dado pessoal, a finalidade, o volume e os riscos do tratamento. A consequência para a biometria é direta: fotografias constantes de documentos públicos não autorizam sua conversão em base universal de identificação policial — exatamente a tese de Doneda de que a visibilidade do dado não afasta o controle do tratamento.¹⁵

Na **ADI 6.529**, o Tribunal rejeitou o acesso indiscriminado a dados em nome da “inteligência estatal”, no contexto do fornecimento de informações do SISBIN à ABIN, cunhando fórmula que dialoga frontalmente com o poder instrumentário: **capacidade tecnológica de acesso não se confunde com competência jurídica de acesso**. O fato de o Estado poder tecnicamente acessar uma base não significa que esteja juridicamente autorizado a fazê-lo.¹⁶

Na **ADI 6.649** e na **ADPF 695**, relativas ao Cadastro Base do Cidadão, o STF admitiu o intercâmbio de informações entre órgãos públicos para a otimização de políticas públicas, mas o condicionou a **finalidade legítima**, minimização da coleta, controle de acesso e responsabilidade informacional. E, na **ADI 5.545**, declarou inconstitucional norma fluminense que impunha a coleta compulsória de material genético de mães e recém-nascidos: **finalidade estatal legítima não torna automaticamente legítimo o tratamento biométrico** — a legitimidade do fim não dispensa o controle constitucional do meio.¹⁷¹⁸

5.2 Controle da atividade política

Na **ADPF 722**, o Supremo julgou inconstitucionais atos do Ministério da Justiça que produziram dossiês sobre integrantes do chamado “movimento antifascista”. A premissa é clara: participar de manifestação lícita não autoriza o Estado a catalogar a orientação política do cidadão. É a versão pública do excedente comportamental de Zuboff: o Estado não pode extrair, da atividade cívica visível, um “excedente” de classificação política.¹⁹

15. Cf. STF, ADIs 6.387, 6.388, 6.389, 6.390 e 6.393 (MC-Ref.), Rel. Min. Rosa Weber, Plenário, j. 07/05/2020 (suspensão da MP nº 954/2020). Correlativamente, Cf. Doneda, 2006.

16. Cf. STF, ADI 6.529/DF, Rel. Min. Cármen Lúcia, Plenário, medida cautelar referendada em 13/05/2020.

17. Cf. STF, ADI 6.649/DF e ADPF 695/DF, Rel. Min. Gilmar Mendes, Plenário, j. 15/09/2022 (Decreto nº 10.046/2019 — Cadastro Base do Cidadão).

18. Cf. STF, ADI 5.545/RJ, Rel. Min. Luiz Fux, Plenário, j. 13/04/2023, unânime.

19. Cf. STF, ADPF 722/DF, Rel. Min. Cármen Lúcia, Plenário, j. 13/05/2022. Correlativamente, Cf. Zuboff, 2021.

5.3 Controle da atividade policial

Na **ADPF 635**, o STF reconheceu um “estado de coisas ainda inconstitucional” na segurança pública fluminense e determinou GPS, câmeras corporais e gravação em viaturas. Dessa decisão extrai-se distinção decisiva entre dois vetores da tecnologia: a **câmera corporal** documenta a atuação policial e reduz a assimetria de poder entre Estado e cidadão; o **reconhecimento facial**, ao contrário, identifica toda pessoa no espaço público e aumenta essa assimetria. Registre-se o dado do Instituto Igarapé: os direitos mais atingidos são os da população negra, em particular jovens negros, e sistemas de reconhecimento facial já justificaram prisões de inocentes.²⁰

5.4 Controle antidiscriminatório

Na **ADPF 186**, o STF admitiu a classificação racial pelo Estado em políticas afirmativas (heteroidentificação), desde que respeitadas a dignidade, o contraditório e **critérios controláveis**. A inferência é poderosa: se até a classificação racial benigna exige controlabilidade, a classificação algorítmica que desencadeia abordagem policial não pode operar como “caixa-preta” insuscetível de contestação. Quanto à LGPD, o art. 4º, III, exclui sua aplicação integral à segurança pública, mas seus princípios não desaparecem — e a EC 115/2022 elevou a proteção de dados a direito fundamental autônomo.^{21,22}

6. Síntese correlacional: o teste dos doze requisitos e a refutação do argumento da “rua pública”

Da leitura conjunta dos precedentes emerge um teste cumulativo de doze requisitos: **legalidade**, finalidade determinada, necessidade, **proporcionalidade**, minimização, segurança, **transparência**, auditabilidade, **controle humano**, devido processo, igualdade material e não discriminação. Cada requisito neutraliza um vetor específico do poder informacional descrito por Zuboff e disciplinado por Doneda: a finalidade determinada bloqueia a expansão progressiva; a transparência e a auditabilidade rompem o espelho unilateral; o controle humano e o devido processo abrem a caixa-preta; a igualdade material enfrenta o erro, a seleção e o efeito diferenciais.²³

A correlação desarma, por fim, o argumento corrente segundo o qual “não existe privacidade sobre o rosto de quem caminha em rua pública”. Pela lente de Doneda, o problema jurídico não é esconder o rosto, mas o **tratamento biométrico do rosto**: a visibilidade pública do dado não autoriza sua transformação em insumo de siste-

20. Cf. STF, ADPF 635/RJ (“ADPF das Favelas”), Rel. Min. Edson Fachin, Plenário, decisão de mérito concluída em 03/04/2025.

21. Cf. STF, ADPF 186/DF, Rel. Min. Ricardo Lewandowski, Plenário, j. 26/04/2012 (decisão unânime).

22. Cf. art. 4º, III, da Lei nº 13.709/2018 (LGPD); art. 5º, LXXIX, da Constituição (EC nº 115/2022).

23. Cf. Zuboff, 2021; Doneda, 2006. Sobre os precedentes que compõem o “standard”, ver notas 14 a 20. O teste dialoga com a matriz de decisão para os conflitos entre memória e dados proposta na parte 2 deste díptico (item 10.3).

mas de identificação e predição, pois o que se controla não é o segredo, e sim o poder gerado pelo tratamento. Pela lente de Zuboff, esse tratamento é justamente o mecanismo pelo qual a assimetria informacional se converte em assimetria de poder — e é essa conversão que o standard do STF veio conter.²⁴

7. Lógica do tema (Poder informacional e vigilância biométrica estatal)

A lógica do sistema pode ser reconstruída em cadeia. Ponto de partida: a economia digital descobriu que a experiência humana gera um **excedente informacional** apropriável, convertendo dados em predições e predições em lucro e influência (Zuboff). O incentivo estrutural desse modelo conduz da observação à modulação — nasce o poder instrumentário — e produz assimetria radical: a organização tudo vê, o indivíduo nada enxerga.

O direito responde deslocando o eixo da privacidade-segredo para a **proteção de dados como disciplina do poder de tratamento** (Doneda): não importa se a informação é secreta, mas o que se faz com ela; e, porque entregar dados virou condição de cidadania, o consentimento é insuficiente — exigem-se limites objetivos, dados sensíveis reforçados e autoridades independentes.

Quando esse aparato migra para o Estado — reconhecimento facial, bancos biométricos, inteligência de dados -, o risco se agrava: a biometria é imutável, o sistema é opaco e o viés é estrutural. A Constituição então opera em quatro frentes concêntricas fixadas pelo STF: **controle informacional** (finalidade, necessidade, proporcionalidade — ADIs 6.387+, 6.529, 6.649 e 5.545), **controle da atividade política** (ADPF 722), **controle da atividade policial** (tecnologia para vigiar o Estado, não o cidadão — ADPF 635) e **controle antidiscriminatório** (ADPF 186). O fecho é o teste cumulativo de doze requisitos: se qualquer um falhar, o tratamento é inconstitucional, ainda que o fim declarado seja legítimo. Em uma frase: **a legitimidade do fim nunca dispensa o controle constitucional do meio**.

24. Cf. Zuboff, 2021; Doneda, 2006. A mesma lógica opera, na parte 2 deste díptico, sob o nome de fricção informacional (item 8.2): público não significa imediatamente encontrável, como decidiu o TEDH no caso Satakunnan.

8. Quadro Sinótico

TEMA	EXPLICAÇÃO DO INSTITUTO
Perspectiva de Zuboff	Análise de economia política. Descreve a forma de poder que surge quando organizações acumulam capacidade extraordinária de conhecer e influenciar comportamentos humanos em escala massiva.
Perspectiva de Doneda	Análise de direito dogmático. Identifica a estrutura jurídica necessária para proteger a pessoa quando seus dados se tornam elemento permanente de decisões, classificações e relações sociais.
Capitalismo de vigilância	Nova lógica de acumulação econômica: a experiência humana é convertida em matéria-prima informacional. O uso de serviços digitais gera dados necessários ao serviço e, além deles, volume muito maior de informações sobre hábitos, interesses e padrões.
Excedente comportamental	Dados coletados além do necessário à prestação do serviço. São apropriados, processados e convertidos em produtos de predição, comercializados a quem deseja antecipar condutas.
Poder instrumentário	Poder que usa infraestruturas digitais para observar, calcular e orientar comportamentos em grande escala. Substitui o “eu sei o que você fez” pelo “posso modificar o ambiente para aumentar a probabilidade de determinada escolha”.
Espelho unilateral	Metáfora da assimetria estrutural: a organização vê o usuário, mas o usuário não vê o processo de observação, classificação e predição. A assimetria informacional converte-se em assimetria de poder.
Privacidade clássica	Concentra-se na esfera reservada e na proteção contra interferências. Pergunta central: “essa informação é secreta?”.
Proteção de dados pessoais	Categoria autônoma, “herdeira” da privacidade. Disciplina o poder produzido pelo tratamento de informações. Pergunta central: “que tratamento está sendo realizado?”. Pode haver violação sem revelação de segredo.
Autodeterminação informativa	Vai além do consentimento: a pessoa deve ocupar posição juridicamente relevante durante todo o ciclo de tratamento, com poderes de conhecimento, controle e reação. Na biometria, ganha gravidade: o dado é imutável, não pode ser “trocado” como senha.
Quatro gerações de leis	Primeira: controle de grandes bancos de dados estatais. Segunda: poder individual de reação. Terceira: autodeterminação informativa. Quarta: garantias objetivas, dados sensíveis e autoridades independentes.
Vigilância algorítmica	Uso de sistemas computacionais para coletar, cruzar, classificar, inferir e prever comportamentos a partir de grandes bases de dados. Combina IA, “big data” e biometria; converte corpos anônimos em sujeitos identificáveis.
Modalidades biométricas	Autenticação (1:1): verifica se a pessoa é quem afirma ser. Identificação retrospectiva (1:N): imagem comparada com banco de imagens. Identificação remota em massa (N:N): captação indiscriminada e comparação automática — a forma mais próxima da sociedade de vigilância.

TEMA	EXPLICAÇÃO DO INSTITUTO
Cinco dimensões do problema	Escalabilidade; autodeterminação informativa (biometria imutável, EC 115/2022); opacidade algorítmica; discriminação algorítmica (tecnologia não é neutra); expansão progressiva da finalidade (“function creep”).
“Vigilância negra”	Algoritmos relacionam-se a estruturas históricas de disciplinamento de corpos negros. A desigualdade pode ocorrer antes do erro: concentração de câmeras, composição dos bancos e listas de busca.
Três espécies de discriminação	Erro diferencial: a tecnologia performa desigualmente entre grupos. Seleção diferencial: certos grupos são mais submetidos à tecnologia. Efeito diferencial: a identificação gera consequências desproporcionalmente graves para grupos específicos.
Capacidade técnica x competência jurídica	Fórmula da ADI 6.529: o fato de o Estado poder tecnicamente acessar dados não significa que esteja juridicamente autorizado a fazê-lo.
Dois vetores da tecnologia (ADPF 635)	Tecnologia para controlar o Estado (câmeras corporais: reduz a assimetria de poder) versus tecnologia para vigiar o cidadão (reconhecimento facial em massa: aumenta a assimetria).
LGPD e segurança pública	Art. 4º, III, da LGPD: a lei não se aplica integralmente ao tratamento para segurança pública, mas seus princípios permanecem incidentes; a EC 115/2022 tornou a proteção de dados direito fundamental autônomo (art. 5º, LXXIX).
Standard constitucional	Teste cumulativo de doze requisitos: legalidade; finalidade determinada; necessidade; proporcionalidade; minimização; segurança; transparência; auditabilidade; controle humano; devido processo; igualdade material; não discriminação.
Refutação da “rua pública”	A visibilidade do rosto em espaço público não afasta a tutela: o problema não é esconder o rosto, mas o tratamento biométrico do rosto — isto é, o poder gerado pelo processamento do dado.

9. Tabela de precedentes do STF

ITEM	EXPLICAÇÃO DO PRECEDENTE
ADIs 6.387, 6.388, 6.389, 6.390 e 6.393 (caso IBGE)	Tribunal: STF, Plenário (MC-Referendo). Relatora: Min. Rosa Weber. Julgamento: 07/05/2020. Objeto: MP nº 954/2020, que impunha o compartilhamento de dados de usuários de telefonia com o IBGE. Ratio decidendi: a proteção de dados pessoais é direito fundamental autônomo, extraído da dignidade humana, da privacidade (art. 5º, X) e do habeas data (art. 5º, LXXII); o exame constitucional considera dado, finalidade, volume e riscos; a mera invocação genérica de interesse público é insuficiente. Consequência: fotos em documentos públicos não autorizam base universal policial.

ITEM	EXPLICAÇÃO DO PRECEDENTE
ADI 6.529 (SISBIN/ABIN)	Tribunal: STF, Plenário. Relatora: Min. Cármen Lúcia. Julgamento: medida cautelar referendada pelo Plenário em 13/05/2020, com decisão de mérito posterior no mesmo sentido. Objeto: fornecimento de dados dos órgãos do SISBIN à ABIN (Lei nº 9.883/1999). Ratio decidendi: rejeição do acesso indiscriminado a dados em nome da “inteligência estatal”; capacidade tecnológica de acesso não equivale a competência jurídica de acesso; o compartilhamento exige interesse público comprovado e controles.
ADI 6.649 e ADPF 695 (Cadastro Base do Cidadão)	Tribunal: STF, Plenário. Relator: Min. Gilmar Mendes. Julgamento: 15/09/2022. Objeto: Decreto nº 10.046/2019, sobre compartilhamento de dados na Administração. Ratio decidendi: o intercâmbio de informações é legítimo para otimização de políticas públicas, mas condicionado a finalidade legítima, minimização, controle de acesso e responsabilidade informacional (interpretação conforme).
ADI 5.545 (coleta genética compulsória — RJ)	Tribunal: STF, Plenário. Relator: Min. Luiz Fux. Julgamento: 13/04/2023, por unanimidade. Objeto: norma fluminense que determinava coleta compulsória de material genético de mães e bebês no parto. Ratio decidendi: finalidade estatal legítima não torna automaticamente legítimo o tratamento biométrico; a legitimidade do fim não dispensa o controle constitucional do meio.
ADPF 722 (dossiês antifascistas)	Tribunal: STF, Plenário. Relatora: Min. Cármen Lúcia. Julgamento: 13/05/2022. Objeto: atos do Ministério da Justiça que produziram dossiês sobre integrantes do “movimento antifascista”. Ratio decidendi: participar de manifestação lícita não autoriza o Estado a catalogar a orientação política do cidadão; a atividade de inteligência tem limites constitucionais substantivos.
ADPF 635 (ADPF das Favelas)	Tribunal: STF, Plenário. Relator: Min. Edson Fachin. Decisão de mérito concluída em 03/04/2025. Objeto: política de segurança pública do Estado do Rio de Janeiro. Ratio decidendi: reconhecimento de “estado de coisas ainda inconstitucional”; determinação de GPS, câmeras corporais e gravação em viaturas; a tecnologia deve documentar e controlar a atuação estatal, reduzindo a assimetria de poder entre Estado e cidadão.
ADPF 186 (cotas raciais — UnB)	Tribunal: STF, Plenário. Relator: Min. Ricardo Lewandowski. Julgamento: 26/04/2012, por unanimidade. Objeto: constitucionalidade das cotas raciais na UnB. Ratio decidendi: a classificação racial pelo Estado é admissível em políticas afirmativas, desde que respeite dignidade, contraditório e critérios controláveis. Inferência para o tema: classificação algorítmica que desencadeia abordagem policial não pode operar como “caixa-preta” insuscetível de contestação.

Referências

- BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988.
- BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Inclui a proteção de dados pessoais entre os direitos e garantias fundamentais. Brasília, DF, 2022.
- BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018.

BRASIL. Supremo Tribunal Federal. ADI 5.545/RJ. Plenário, 2023.

BRASIL. Supremo Tribunal Federal. ADIs 6.387, 6.388, 6.389, 6.390 e 6.393 (MC-Ref.).
Relatora: Min. Rosa Weber. Plenário, julgadas em 7 maio 2020.

BRASIL. Supremo Tribunal Federal. ADI 6.529/DF. Relatora: Min. Cármen Lúcia. Plenário.

BRASIL. Supremo Tribunal Federal. ADI 6.649/DF e ADPF 695/DF. Relator: Min. Gilmar
Mendes. Plenário.

BRASIL. Supremo Tribunal Federal. ADPF 186/DF. Relator: Min. Ricardo Lewandowski.
Plenário, julgada em 26 abr. 2012.

BRASIL. Supremo Tribunal Federal. ADPF 635/RJ. Relator: Min. Edson Fachin. Plenário, 2025.

BRASIL. Supremo Tribunal Federal. ADPF 722/DF. Relatora: Min. Cármen Lúcia. Plenário.

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

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço
Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

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