



Vereadora Janaina Paschoal (PP)

PROJETO DE LEI Nº ____/2025

Dispõe sobre a proteção de dados biométricos no âmbito da Cidade de São Paulo e dá outras providências.

Art. 1º A coleta de dados biométricos, no Município de São Paulo, observará os princípios da Lei Geral de Proteção de Dados, em especial a necessidade estrita, a proporcionalidade, o dever de informar e a autodeterminação do titular.

Art. 2º Fica proibido, no Município de São Paulo, o escaneamento de íris.

Art. 3º Fica proibida, no Município de São Paulo, a coleta de dados biométricos como condição de acesso a prédios, estabelecimentos, eventos e elevadores, independentemente de serem públicos ou privados.

§ 1º - Para os fins desta lei, consideram-se dados biométricos as impressões digitais, o reconhecimento facial, a íris, a voz e demais marcadores que possam constituir identificação única.

§ 2º - A apresentação de documento de identificação poderá ser solicitada, mas a retenção do documento não será admitida.

§ 3º - Fotografia digital poderá ser retirada.

Art. 4º O disposto nesta lei não inviabiliza o reconhecimento facial pautado na identificação de pessoas cujos dados já integrem os sistemas policiais e judiciais criminais.

Art. 5º Fica proibido, no Município de São Paulo, inserir chips cerebrais em seres humanos, salvo para fins de tratamento de saúde, sob indicação de, pelo menos, dois médicos.

Art. 6º Fica proibido, no Município de São Paulo, monitorar o cérebro de seres humanos em tempo real, para qualquer fim.

Parágrafo único- A vedação do caput não se aplica a exames solicitados por médicos, objetivando diagnóstico e tratamento de saúde.

Art. 7º O Poder Executivo poderá regulamentar esta Lei no que couber, especialmente quanto aos procedimentos de fiscalização e aplicação de sanções.

Art. 8º Esta Lei entra em vigor na data de sua publicação.

São Paulo, 5 de fevereiro de 2026.

Janaina Paschoal
Vereadora PP



**CÂMARA MUNICIPAL DE
SÃO PAULO**

Vereadora Janaina Paschoal (PP)

Justificativa

Esta parlamentar, já há um bom tempo, tem se preocupado com o tema da proteção de dados, com destaque para os biométricos. Não só em decorrência de sua condição de Presidente da Comissão Parlamentar de Inquérito do escaneamento de íris e Professora de Direito, mas também de cidadã, reiteradamente compelida a fornecer dados sensíveis para acessar portarias de edifícios (públicos e privados), hotéis e elevadores.

Tais coletas, em regra, são realizadas sem informações claras sobre a finalidade, o tempo de armazenamento ou as medidas de segurança adotadas. A bem da verdade, sequer resta demonstrada a real necessidade de captar informações tão invasivas.

Com efeito, os dados são desproporcionalmente retidos, até mesmo para simples circulação em ambientes públicos, prática que vem se naturalizando sem a devida reflexão. A ora signatária jamais vai esquecer a indignação que experimentou quando, no início do mandato, ao ingressar em um prédio público, fora instada a registrar as digitais dos dez dedos das mãos.

Talvez as pessoas não se sintam tão invadidas, por não terem vivenciado os debates jurídicos dos anos 90, quando investigados pelos mais graves crimes tinham “habeas corpus” impetrados em seu favor, para impedir indiciamento por meio de identificação criminal, uma vez que a Constituição Federal, em seu artigo 5º., inciso LVIII, garante que a identificação civil afasta a necessidade de fornecer digitais.

Em outras palavras, passados alguns anos daquelas intensas discussões, ninguém parece estranhar precisar mostrar identidade, registrar digitais, retirar fotografia, às vezes até conjuntamente, apenas para ingressar em um edifício!

O fato de as pessoas terem se “acostumado” a essa dinâmica pode explicar a absoluta ausência de reação à instalação de uma empresa estrangeira na Capital, com múltiplas unidades nos mais diversos bairros, objetivando escanear a íris dos paulistanos e de todos os indivíduos que ousassem passar pela frente de uma dessas tais “lojinhas”, sem maiores explicações acerca dos reais objetivos.

Não fosse a atuação firme desta Câmara, que autorizou renovar o prazo da Comissão Parlamentar de Inquérito antes mencionada, talvez os dados de nossos cidadãos ainda estivessem sendo indiscriminadamente coletados e encaminhados a instituições estrangeiras, sem maiores pudores.

É bem verdade que a Autoridade Nacional de Proteção de Dados, agora Agência Nacional de Proteção de Dados, proibiu a remuneração pelo escaneamento de íris, reduzindo significativamente a atuação da empresa nesta Cidade; entretanto, não houve vedação à prática propriamente dita.

Ao longo dos trabalhos da Comissão Parlamentar de Inquérito, muitos ofícios foram expedidos, muitas pessoas foram ouvidas. Incrivelmente, constatou-se que a empresa estrangeira, que escaneou mais de meio milhão de íris de cidadãos, sequer possui CNPJ no Brasil. Aliás, até mesmo aqueles que se apresentam como seus representantes foram contratados por empresas intermediárias. Mas não é só! As pessoas jurídicas responsáveis pela locação dos espaços em que funcionaram as várias “lojinhas” foram contratadas pela empresa estrangeira, que não assinou nenhum contrato referente à operação no Brasil, sendo certo que seus funcionários também foram selecionados e pagos por terceiros.



Vereadora Janaina Paschoal (PP)

Como se não bastasse, a tal empresa criou uma “moeda” própria, fazendo pagamentos, estabelecendo negociações e criando um ambiente digital para a utilização dessa sua moeda. Os desafios éticos e jurídicos desse novel modelo são gigantescos e serão abordados na seara adequada.

Não obstante, já há elementos suficientes a alicerçar a apresentação deste projeto de lei, com o objetivo de deixar bem claro que, no Município de São Paulo, o escaneamento de íris não será tolerado, não se admitindo, igualmente, a captação desenfreada de outros dados biométricos para os atos mais simplórios da vida quotidiana.

A justificar a medida, para além da proteção da intimidade e da privacidade, pilares constitucionais, há a prevenção ao risco de vazamentos, com as muitas consequências deletérias já conhecidas e outras tantas, ainda sequer imaginadas.

A título de exemplo, recorda-se que, no Afeganistão, o grupo Talibã utilizou bases de dados vazadas para perseguir dissidentes e opositores. Os dados eram provenientes de um programa do próprio governo afegão para emissão de identidade eletrônica, mas em posse dos terroristas, tornou-se potente instrumento de controle e submissão. (Disponível em: <https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans#:~:text=The%20Taliban%20have%20previously%20used,dangerous%20than%20they%20were%20helpful.%E2%80%9D>).

Muito embora, a princípio, o presente projeto tenha finalidades mais simplórias que a de proteger os cidadãos do terrorismo, imperioso observar que a exigência de dados biométricos como condição para ingresso em condomínios, estabelecimentos, repartições públicas, elevadores, dentre outros, cria um *consentimento coagido*, pois o titular teoricamente poderia recusar a submissão à captação; entretanto, na prática, a negativa impediria sua circulação e o acesso a direitos básicos, convertendo essa “escolha” em obrigação disfarçada.

Tal cenário viola a autodeterminação, que pressupõe decisão livre, informada e reversível, e se agrava quando a coleta biométrica é desproporcional à finalidade, ou seja, quando existem meios menos invasivos que poderiam atender ao mesmo objetivo. A adoção rotineira desse modelo não apenas amplia a indesejável vigilância cotidiana, mas alimenta bancos centralizados de biometria, cuja existência eleva o risco sistêmico: Um único vazamento ou mau uso passa a expor permanentemente as identidades de muitos cidadãos, sem possibilidade de substituição ou reparação efetiva.

Vale ressaltar que a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) classifica dados biométricos, identificadores, como **sensíveis**, sujeitos a tratamento mais rigoroso justamente por representarem uma dimensão permanente e inseparável do titular. Os princípios basilares do tratamento de dados estão expressos nos artigos 2º. e 6º da lei, dentre os quais, destacam-se: I -) finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II -) adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; e III -) necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. Em resumo, é preciso que haja PROPORCIONALIDADE!

Estivesse esta Parlamentar no Congresso Nacional, certamente, o projeto de lei apresentado traria maiores vedações. No âmbito municipal, em decorrência dos limites de atribuição, a proposição ora apresentada aos pares, cinge-se a tornar mais concretos os princípios acima para o



Vereadora Janaina Paschoal (PP)

Município de São Paulo, que é uma Cidade-Estado e, por conseguinte, alvo constante de abusos na seara de captação e tratamento de dados biométricos, para fins nem sempre tão claros.

Os princípios protegidos pela LGPD, reforçados no presente projeto de lei, estão em consonância com leis, projetos e discussões havidas em todo o mundo.

Na União Europeia, o Regulamento Geral de Proteção de dados (GDPR) confere forma clara ao conceito de “minimização dos dados” (Art 5. 1. c), relacionado aos princípios de necessidade e proporcionalidade. De onde se depreende que, na possibilidade de coleta parcial de informação biométrica para cumprir certo propósito, não se deve coletar a totalidade dos dados. Sendo suficiente à finalidade a coleta da digital de apenas um dedo, não há motivo para reter informações dos dez dedos.

Igualmente, o *Universal Digital Public Infrastructure Safeguards Framework Recommendations* assegura que as autenticações biométricas não sejam obrigatórias, havendo sempre medidas alternativas ao fornecimento de dados biométricos sensíveis. Conferir em: <https://www.dpi-safeguards.org/>

A legislação argentina de proteção de dados, Lei nº 25.326/00, em seu Artigo 4º, estabelece que os dados coletados devem ser pertinentes, adequados e não excessivos em relação à finalidade que motivou sua obtenção, alinhando-se ao princípio da minimização presente na LGPD e no GDPR.

Os Estados Unidos, por sua vez, não possuem uma única lei de proteção de dados abrangente como a LGPD no Brasil, mas sim um conjunto de leis federais e estaduais que regulam diferentes aspectos da privacidade. Cabe mencionar, entretanto, a existência de um projeto para o tratamento de dados biométricos em tramitação. Trata-se do *National Biometric Information Privacy Act of 2020*. Disponível em: <https://www.congress.gov/bill/116th-congress/senate-bill/4400>

As leis estadunidenses firmam elementos recorrentes como consentimento, retenção mínima, destruição, proibição de comercialização e informação por escrito das ações ao titular.

A lei do Estado de Illinois, *Biometric Information Privacy Act - BIPA*, foi uma das pioneiras na regulamentação do tratamento de informações biométricas. No texto sancionado em 2008, define-se o conceito de identificador biométrico e instituem-se obrigações legais para coleta, captura e recebimento destes identificadores. O Ato também obriga ao coletor dos dados manter uma política explícita e determinada de retenção e destruição dos identificadores, sendo que estes devem ser destruídos após a finalidade alcançada ou dentro de um prazo máximo de 3 anos da coleta. É também vedada a venda, aluguel ou qualquer meio de obtenção de lucro com os identificadores, sendo que a divulgação e compartilhamento são delimitados a determinadas circunstâncias, como consentimento explícito, transação financeira ou ordem judicial. Esta lei também prevê um direito de ação a quaisquer pessoas que eventualmente fossem prejudicadas pela violação e as penalidades do texto original variam de mil a cinco mil dólares. Conferir em: <https://www.ilga.gov/Legislation/ILCS/Articles?ActID=3004&ChapterID=57>

Os estados do Texas e Califórnia também têm suas próprias regulações no que se refere aos dados biométricos, ambos estados de grande relevância para o desenvolvimento do setor digital devido à concentração de empresas globalmente importantes para o meio.

No Texas, vigora uma lei enxuta e concisa, o *Capture or Use of Biometric Identifier Act*, que veda a venda ou aluguel de dados sem o consentimento do titular e prevê a destruição do identificador após um prazo razoável, sendo o máximo período de 1 ano após a coleta ou quando



Vereadora Janaina Paschoal (PP)

terminado o contrato se for para um propósito de segurança por parte de um empregador. Conferir em: <https://www.texasattorneygeneral.gov/consumer-protection/file-consumer-complaint/consumer-privacy-rights/biometric-identifier-act>

A legislação da **Califórnia** sobre o assunto é consideravelmente mais longa, integrando um conjunto de atos de defesa do consumidor. As seções que tratam principalmente do tema respondem pelos números de 1798.100 até 1798.120. Apesar de não proibir a venda de dados biométricos, dá ao consumidor o direito de requerer que seu identificador não seja vendido. Disponível em:

https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

A lei de identificadores biométricos do estado de Washington tem um foco especial nas condições do consentimento, afirmando textualmente que a mera notificação não pode ser considerada consentimento afirmativo e este depende sobremaneira do contexto em que é obtido. Esta lei também proíbe a venda, aluguel ou divulgação do dado biométrico sem consentimento, tal como as outras, requer que o dado só pode ser retido pelo tempo necessário para se cumprir a finalidade, embora não estipule prazo máximo. Disponível em: <https://app.leg.wa.gov/RCW/default.aspx?cite=19.375&full=true&utm>

O estado de Nova York implementou seu *Biometric Privacy Act* em 2021, exigindo que entidades privadas que possuam identificadores biométricos desenvolvam uma política escrita estabelecendo um cronograma de retenção e diretrizes para destruir permanentemente estes identificadores quando o propósito inicial de coletar tais informações tiver sido cumprido ou dentro de três anos após a última interação do indivíduo com a entidade. Disponível em: https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=A00027&term=2021&Summary=Y&Text=Y

A Cidade de Nova York também tem discutido o tema, com dois projetos em tramitação. O **Int 0217-2024**, que pretende tornar ilegal, para qualquer estabelecimento aberto ao público, usar tecnologia de reconhecimento biométrico para identificar um cliente sem consentimento (<https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=6557556&GUID=E67A1D7D-5245-4373-B5FF-1AD968E3383F>) e o **Int 0425-2024**, que impede um condomínio residencial de instalar tecnologia de reconhecimento biométrico que identifique inquilinos ou convidados de um inquilino (<https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=6558031&GUID=73676D60-2010-4A95-AB2F-A0B96A46C45E>).

Outras localidades ainda expressam preocupações semelhantes, como é o caso da cidade de **Portland**, que proibiu, nos idos de 2021, o uso de tecnologias de reconhecimento facial por entidades privadas em locais de acesso público. Conferir em: <https://www.portland.gov/code/34/10>

O estado canadense do Québec pode ser considerado um modelo de maior controle e prevenção de riscos, pois tem o que provavelmente é a ação protetiva mais rigorosa, requerendo que qualquer entidade que pretenda criar uma base com dados biométricos deve comunicar à comissão responsável em um prazo máximo de 60 dias antes do começo do funcionamento (p.29, item 77). Disponível em: <https://www.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html>

Encontra-se na própria página da *Commission D'accès à L'information*, autoridade responsável pelo controle das autorizações, o seguinte informativo: “Qualquer pessoa que deseje utilizar dados biométricos é obrigada a divulgá-los à Comissão se: verifica ou confirma a



Vereadora Janaina Paschoal (PP)

identidade por meio de um processo que permite a captura de características ou medidas biométricas; cria um banco de dados de características ou medidas biométricas – neste caso, a divulgação deve ser feita pelo menos 60 dias antes da entrada em funcionamento do banco.”. Conferir em: <https://www.cai.gouv.qc.ca/protection-renseignements-personnels/sujets-et-domaines-dinteret/biometrie>

Até mesmo a China, país não democrático, responsável pelo desenvolvimento de grande parte da tecnologia de reconhecimento pessoal, em 2025, adotou salvaguardas claras em relação à instalação de redes de reconhecimento para seus cidadãos, estabelecendo que a tecnologia deve seguir o critério da necessidade, bem como que nenhuma organização pode enganar, fraudar ou mesmo coagir indivíduos a aceitarem a tecnologia de reconhecimento facial para verificação de identidade, sendo certo que tal identificação facial não pode ser utilizada como método exclusivo, devendo alternativas serem disponibilizadas. Conferir em: https://www.cac.gov.cn/2025-03/21/c_1744174262156096.htm

A expansão silenciosa, muitas vezes desenfreada, de sistemas de reconhecimento facial, impressões digitais e outros identificadores corporais em condomínios, repartições públicas e espaços privados de uso coletivo tem contribuído para formar bancos de dados permanentes e sem proteção adequada, com informações fundamentais relacionadas à identidade humana.

Importante consignar que diferentemente de senhas e documentos, sejam físicos ou digitais, características corporais não podem ser recriadas ou substituídas quando expostas, tornando a biometria mais que um simples dado pessoal, mas um vetor permanente de identificação. Esse fato foi corroborado pelo Defensor Público Thomaz Fiterman Tedesco, Coordenador do Grupo instituído, no âmbito da Defensoria, para investigar o escaneamento de íris no Município de São Paulo, em depoimento prestado à Comissão Parlamentar de Inquérito, no dia 03 de fevereiro do ano corrente. Conferir em: https://www.youtube.com/watch?v=OLEMwgow_vc&list=PLyt3a0f9wjCkHNjd8mLj5JGIFGY5zArJO.

É bem verdade que existe uma consonância de aspectos das diversas leis de proteção de dados, mesmo em diferentes países: o esforço no sentido de limitar o poder de vigilância do Estado e de entidades privadas sobre o indivíduo. Essas normas reconhecem a biometria como dado sensível e, portanto, sujeito à proteção reforçada, exigindo justificativa clara, finalidade legítima e consentimento válido para o seu tratamento. Ainda assim, o que deveria ser exceção (coleta e uso de dados biométricos) tornou-se procedimento cotidiano, aplicado como barreira de acesso a lugares e serviços, sem nenhuma justificativa, necessidade ou proporcionalidade. Notável, portanto, o distanciamento entre a proteção jurídica teórica e a realidade. Daí o cabimento do presente projeto de lei que, em poucos artigos, de forma clara e objetiva, no Município de São Paulo, protege os indivíduos do escaneamento de íris, bem como da imposição de fornecimento de dados biométricos para o simples acesso a prédios, estabelecimentos e elevadores.

A análise dos muitos diplomas já vigentes e em tramitação ao redor do mundo evidencia uma larga gama de definições do que sejam dados biométricos. Nesta oportunidade, a fim de evitar polêmicas e questionamentos jurídicos, elegeu-se uma definição mais singela e objetiva, exclusivamente para dar concretude às vedações que se pretendem estabelecer por meio da norma a que ora se roga o apoio dos pares. Por isso, no parágrafo primeiro do artigo terceiro, consignase, textualmente, que para os fins da lei proposta consideram-se dados biométricos as impressões digitais, o reconhecimento facial, a íris, a voz e demais marcadores que possam constituir identificação única.



**CÂMARA MUNICIPAL DE
SÃO PAULO**

Vereadora Janaina Paschoal (PP)

Insta reforçar que biometria não é apenas um recurso tecnológico neutro! Quando o acesso ao ambiente físico passa a ser condicionado ao fornecimento de características corporais imutáveis, consolida-se uma relação desigual entre o cidadão e quem detém o banco de dados, sobretudo quando não há opção de recusa ou justificativa proporcional que sustente a exigência. O ser humano passa a ser visto como coisa, como chave, restando instrumentalizado, em situação incompatível com a dignidade humana, constitucionalmente assegurada.

Com efeito, apesar dos limites normativos mencionados, a realidade prática brasileira revela um cenário de expansão acelerada do uso de biometria em espaços públicos e privados, frequentemente sem consentimento livre e informado, e sem quaisquer alternativas menos invasivas, na contramão do entendimento de diversas legislações pelo mundo. Condomínios residenciais condicionam o ingresso de moradores e visitantes ao fornecimento de digitais ou reconhecimento facial, repartições públicas utilizam captura biométrica como critério de autenticação primária, e estabelecimentos comerciais importam soluções de identificação facial para obter agilidade operacional sem, muitas vezes, garantir transparência. É notável também a ausência de exigência efetiva de uma política de retenção ou mecanismos reais de oposição. Na prática, o princípio da necessidade, que deveria exigir que apenas o mínimo indispensável fosse coletado, tem sido flexibilizado, aproximando-se da inexistência.

A LGPD contém os instrumentos necessários para restringir tais práticas, mas sua eficácia requer interpretação estrita, fiscalização ativa e conscientização coletiva sobre o risco de transformar o corpo humano em chave de acesso obrigatória ao convívio social.

A devida proporcionalidade implica que a coleta de dados biométricos deve ser o último recurso e não a primeira opção. A formação de bancos de dados biométricos sem justificativa técnica robusta viola diretamente os princípios estruturantes estabelecidos pela lei federal, daí a necessidade deste projeto de lei.

Por fim, consigna-se que a defesa da privacidade não se confunde com resistência ao progresso, constituindo garantia de que o avanço tecnológico seja acompanhado de prevenção e controle de risco.

Para preservar essa privacidade e prevenir sérios riscos de danos individuais e coletivos, além da proibição do escaneamento de íris e da coleta de dados biométricos para os acessos mais comzeinhos na nossa Cidade, por cautela, o presente projeto de lei também busca, ainda que antecipadamente, vedar o uso de chips cerebrais em seres humanos, ou de quaisquer equipamentos de monitoramento cerebral, para finalidade não médica.

No que concerne aos chips cerebrais, sabe-se que muitas pesquisas já estão em andamento, objetivando desenvolver e aprimorar esses dispositivos a pessoas acometidas por doenças e acidentes neurológicos, viabilizando mobilidade, comunicação e até mesmo trabalho.

A Vereadora proponente, por óbvio, é uma entusiasta desses avanços, até em virtude de ter acompanhado o aprisionamento de seu pai no próprio corpo, por força de uma doença rara intitulada paralisia supranuclear progressiva. No entanto, por estudar e lecionar Bioética e Temas Essenciais à Natureza Humana, há muitos anos, bem sabe que as experiências com seres humanos e o desejo de controle são uma constante na história da humanidade.

No que tange à vedação do monitoramento do cérebro em tempo real, muito embora ainda não presente na vida nacional, já é uma realidade em algumas nações, como a China, onde escolas e empresas se valem de capacetes com eletrodos, sob o pretexto de segurança dos estudantes e trabalhadores.



**CÂMARA MUNICIPAL DE
SÃO PAULO**

Vereadora Janaina Paschoal (PP)

A segurança, nas mais diversas searas, é muito importante, não se pode negar; porém, a busca por absoluta segurança não pode justificar todo tipo de interferência, seja captando os dados biométricos dos indivíduos, seja monitorando seus cérebros, com dispositivos internos, ou externos.

A prova de que esta Parlamentar preza pela segurança está na previsão expressa de que as proibições constantes da lei proposta não prejudicam os sistemas de reconhecimento facial, pautados em bancos de dados policiais e da justiça criminal, como são os casos do Muralha e do Smart Sampa.

Tal excludente não se alicerça em preferências políticas, mas no pilar, presente em vários ordenamentos, de que os reconhecimentos em ambientes públicos não devem ocorrer de forma ampla e irrestrita; partindo apenas das pessoas já identificadas, ou procuradas, por alguma ação específica, que façam parte dos bancos de dados oficiais do sistema repressivo penal, como, aliás, resta permitido pela Portaria 961/25 do Ministério da Justiça.

Esta Vereadora roga o apoio dos pares, esclarecendo se tratar de projeto vanguardista, na medida em que vem concretizar, não só a Lei Geral de Proteção de Dados, mas também, e principalmente, a própria Emenda Constitucional n. 115/22, que incluiu no Artigo 5º, da Constituição Federal, o inciso LXXIX, segundo o qual resta assegurado “o direito à proteção dos dados pessoais, inclusive nos meios digitais”.

São Paulo, 5 de fevereiro de 2026.

Janaina Paschoal
Vereadora PP