REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

BIOMETRIA FACIAL NA ADMINISTRAÇÃO PÚBLICA: DA EXCEPCIONALIDADE AO COTIDIANO

FACIAL BIOMETRICS IN PUBLIC ADMINISTRATION: FROM EXCEPTIONALITY TO EVERYDAY LIFE

Ciências Sociais Aplicadas • 17/05/2026

REGISTRO DOI: 10.70773/revistatopicos/778869058

Maria Helena de Souza Marques Carneiro

RESUMO

O artigo analisa a expansão do uso da tecnologia de reconhecimento facial pela Administração Pública à luz do direito fundamental à proteção de dados pessoais e dos princípios de tratamento previstos na Lei Geral de Proteção de Dados Pessoais (LGPD), em especial o princípio da necessidade. Para tanto, adota abordagem qualitativa e método hipotético-dedutivo, com revisão bibliográfica e legislativa, complementada pela análise dos casos do Metrô de São Paulo, do sistema de transporte público do Distrito Federal e das escolas públicas do Paraná. Sustenta-se que o tratamento de dados biométricos faciais exige demonstração concreta da indispensabilidade da medida e da inexistência de meios menos invasivos. Conclui-se que a eficiência administrativa não constitui fundamento suficiente para legitimar tratamentos incompatíveis com a proteção de dados pessoais e a autodeterminação informativa.

Palavras-chave: Biometria facial; Proteção de dados pessoais sensíveis; LGPD; Administração Pública; Princípio da necessidade.

ABSTRACT

This article analyzes the expansion of the use of facial recognition technology by the Public Administration in light of the fundamental right to the protection of personal data and the principles of processing provided for in the General Data Protection Law (LGPD), especially the principle of necessity. To this end, it adopts a qualitative approach and a hypothetical-deductive method, with bibliographic and legislative review, complemented by the analysis of the cases of the São Paulo Metro, the public transport system of the Federal District and the public schools of Paraná. It argues that the processing of facial biometric data requires concrete demonstration of the indispensability of the measure and the non-

existence of less invasive means. It concludes that administrative efficiency does not constitute a sufficient basis to legitimize processing incompatible with the protection of personal data and informational self-determination.
Keywords: Facial biometrics; Protection of sensitive personal data; LGPD; Public Administration; Principle of necessity.

1. INTRODUÇÃO

A nova revolução industrial, iniciada na virada do século, transformou profundamente as formas de viver, se relacionar e consumir na sociedade contemporânea. Esse processo é marcado pela rapidez, ubiquidade e mobilidade proporcionadas pela internet[1], que se tornou infraestrutura essencial da vida social, econômica e cultural, a ponto de ser difícil imaginar a existência fora do ambiente digital.

Nesse contexto, a identificação biométrica ganhou destaque como método de autenticação tanto no âmbito público quanto no privado. No Brasil, desde 2008[2], a Justiça Eleitoral passou a utilizar dados biométricos para o reconhecimento do eleitor, inicialmente em caráter experimental, com a coleta de impressões digitais e fotografia, posteriormente consolidada como instrumento de validação da identidade e de prevenção a fraudes no processo eleitoral.

Nos anos seguintes, a identificação biométrica expandiu-se rapidamente para diferentes setores, deixando de se restringir a contextos excepcionais de segurança. Inicialmente associada ao monitoramento em grandes eventos, como a Copa do Mundo de 2014[3] e os Jogos Olímpicos de 2016[4], a tecnologia passou a integrar

atividades ordinárias de autenticação, segurança e controle, a exemplo do show da cantora Lady Gaga em 2025[5], a criação da Identificação Civil Digital (ICD) [6], em 2017, a prova de vida digital do INSS, em 2020[7], e a emissão da nova Carteira de Identidade Nacional, em 2022[8].

Mesmo após a promulgação da Lei Geral de Proteção de Dados – LGPD, que enquadra as informações biométricas como sensíveis[9] e, portanto, sujeitas a um regime jurídico de tutela reforçada, não se verificou retração no emprego de tecnologias de reconhecimento facial. Pelo contrário, sua aplicação intensificou-se em atividades cotidianas, chegando a substituir métodos convencionais, como a chamada escolar, o que revela um descompasso entre a prática administrativa e a natureza especialmente protegida de tais ativos informacionais

Diante desse panorama, o presente artigo analisa o emprego do reconhecimento facial pela Administração Pública sob a ótica do direito fundamental à proteção de dados e dos princípios da finalidade e da necessidade. Com isso, busca-se examinar em que medida a promessa de eficiência administrativa legitima o tratamento, identificando os limites jurídicos impostos à atuação estatal.

Para tanto, adota-se uma abordagem qualitativa e teórico-analítica, fundamentada no método hipotético-dedutivo. A hipótese central sustenta que a expansão da biometria facial para atividades administrativas ordinárias pode configurar violação aos princípios da necessidade e do direito fundamental à proteção de dados. A pesquisa abrange o exame bibliográfico, legislativo e jurisprudencial,

além da análise de casos concretos selecionados para fins de densificação do estudo.

2. BIOMETRIA FACIAL: CONCEITO, FUNCIONAMENTO E RISCOS

A biometria facial pode ser definida como uma espécie de dado pessoal sensível, resultante do processamento técnico de características biológicas convertidas em uma representação matemática singular, o chamado modelo biométrico facial (template facial) [10]. Sob a ótica legislativa nacional, nota-se uma lacuna conceitual, visto que nem o Marco Civil da Internet (Lei n. 12.965/2014) nem a Lei Geral de Proteção de Dados (Lei n. 13.709/2018) fornecem uma definição pormenorizada do termo.

No cenário internacional, o pioneiro Biometric Information Privacy Act[11] (BIPA) restringe-se a incluir o "escaneamento da geometria facial" (scan of face geometry) no rol de identificadores biométricos, equiparando-o, para fins conceituais, à dactiloscopia e ao escaneamento de íris. De modo análogo, o GDPR[12] enquadra os dados biométricos como categoria especial de dados pessoais, contudo, sem esmiuçar as particularidades estruturais da face.

Esse tratamento genérico mostra-se insuficiente diante da complexidade do tema. Diferente de outros identificadores, o rosto humano permite a extração simultânea de múltiplos atributos, tais como origem étnica, faixa etária, padrões de íris e até estados emocionais (Emotion AI[13]). Tal característica amplia exponencialmente o potencial inferencial da biometria facial, transformando o que seria uma simples ferramenta de autenticação em um mecanismo de análise comportamental e demográfica.

Vale ressaltar, que os sistemas de reconhecimento facial operam, via de regra, por meio de técnicas de Inteligência Artificial baseadas em aprendizado de máquina, especificamente modelos de *deep learning* estruturados em redes neurais profundas. Tais arquiteturas são treinadas com vastos conjuntos de dados para identificar padrões e gerar representações matemáticas aptas a reconhecer ou comparar faces sob variáveis angulações, condições de luminosidade e expressões, elevando consideravelmente a acurácia da identificação.

Nesse sentido, a biometria facial apresenta particularidades que impõem um tratamento jurídico mais rigoroso em face de outras modalidades biométricas. Diferentemente da dactiloscopia, que pressupõe contato físico e incide sobre um ponto corporal isolado, o reconhecimento facial viabiliza a captura à distância e prescinde da cooperação ativa do titular. Essa transfiguração do rosto em uma fonte contínua de coleta informacional permite não apenas a autenticação, mas a categorização de indivíduos por atributos como idade, gênero e etnia, além da extração de inferências emocionais e preditivas, frequentemente realizadas sem o consentimento ou ciência do titular.

Soma-se a isso a sua relativa imutabilidade: uma vez comprometido o dado biométrico facial, não há possibilidade prática de substituição equivalente à redefinição de uma senha, o que amplifica o potencial lesivo de vazamentos, fraudes e usos secundários indevidos. Outro diferencial reside na ocorrência de falsos positivos e falsos negativos, falhas inerentes aos sistemas de reconhecimento facial que evidenciam riscos jurídicos e sociais distintos[14].

O falso positivo ocorre quando o sistema vincula indevidamente um indivíduo ao *template* biométrico de outrem, permitindo acessos indevidos e identificações errôneas com potencial discriminatório e repressivo. Já o falso negativo, por sua vez, consiste na rejeição indevida de um usuário legitimamente cadastrado, impedindo seu acesso a serviços ou benefícios essenciais[15].

Desta forma, a implementação de sistemas de reconhecimento facial pela Administração Pública demanda escrutínio rigoroso quanto aos impactos nos direitos fundamentais à proteção de dados, à intimidade e à privacidade. A atividade administrativa, pautada pelos princípios da publicidade e da eficiência, deve equilibrar o avanço tecnológico com uma atuação transparente e proporcional. Tal ponderação entre meios e fins assegura a integridade do ordenamento, impedindo que a busca pela otimização burocrática resulte em retrocesso nas garantias individuais.

3. CASOS EMBLEMÁTICOS DE USO DA BIOMETRIA FACIAL NA ADMINISTRAÇÃO PÚBLICA

No âmbito do Direito Administrativo, o emprego da tecnologia biométrica facial é pautado pela finalidade do tratamento, cujas aplicações variam entre controle de acesso, prevenção a fraudes e monitoramento de indivíduos. Por conseguinte, a mera subsunção do tratamento a uma obrigação legal não se mostra suficiente, porquanto cabe ao agente público analisar a compatibilidade do caso concreto com o regime constitucional e legal de proteção de dados pessoais.

Com base nisso, foram selecionados três casos emblemáticos: metrô de São Paulo, sistema de transporte público do Distrito Federal e escolas públicas do Paraná, com o intuito de verificar a conformidade dessas práticas aos princípios da finalidade e da necessidade, sobretudo diante da justificativa recorrente de eficiência da atividade administrativa.

3.1. Caso do Metrô de São Paulo – Concessionária Viaquatro

Em 2018, a concessionária ViaQuatro utilizou o sistema de Portas Interativas Digitais equipado com câmeras capazes de analisar o gênero, a faixa etária, emoções, além do tempo de atenção dos usuários do metrô, a fim de extrair dados estatísticos publicitários e comerciais. Tudo, porém, sem o consentimento do titular dos dados.

Submetido à apreciação judicial, a concessionária foi condenada a abster de captar imagens, sons ou quaisquer outros dados pessoais dos consumidores-usuários por meio de câmeras ou outros dispositivos, sem o consentimento expresso do titular. Em segundo grau, houve a majoração do valor dos danos morais coletivos de R$ 100.000,00 para R$ 500.000,00, em razão da lesão à intimidade da população usuária do metrô[16].

O caso é tido como o pioneiro sobre judicialização de demandas que envolvam a tecnologia de reconhecimento facial[17]. Embora anterior à plena vigência da LGPD[18], a norma foi utilizada pelo Tribunal como um vetor interpretativo, essencial para os conceitos de dados pessoais sensíveis e da estrutura necessária ao seu tratamento[19]. Nele, estabeleceu-se que a coleta e a análise de imagens faciais para fins comerciais, ainda que sob o argumento de geração de

estatísticas, configuram tratamento de dados biométricos e impõem regime de tutela reforçada.

Outro aspecto relevante reside no fato de que a coleta e o processamento de imagens foram realizados por uma concessionária privada na prestação de um serviço público essencial, porém com finalidade comercial voltada à publicidade direcionada. Essa dinâmica alinha-se à perspectiva de Pasquale[20], para quem a governança contemporânea é exercida por atores que transitam entre as esferas pública e privada, explorando ativos informacionais para fins econômicos e estratégicos.

Essa configuração formada por "agentes híbridos" não neutraliza a lógica econômica subjacente ao tratamento de dados. Sob essa ótica, o processamento não pode ser fundamentado em obrigação legal ou execução de políticas públicas quando dissociado do interesse coletivo primário, sob pena de evidente desvio de finalidade. Ademais, a opacidade no tratamento compromete a segurança dos usuários do serviço público, os quais acabam reduzidos a meros ativos informacionais à disposição do mercado.

3.2. Caso do Transporte Gratuito DF

Em 2018, o Distrito Federal estabeleceu a obrigatoriedade do uso de biometria facial pelos delegatários serviço de transporte público coletivo, como estratégia de combate a fraudes nas gratuidades do Passe Livre Estudantil e de Pessoas com Deficiência. A medida, aplicada a todo o Sistema de Bilhetagem Automática (SBA), fundamenta-se na necessidade de aperfeiçoar a fiscalização dos benefícios tarifários.

Mas como funciona? O sistema realiza a captura das imagens faciais dos usuários no momento da validação do cartão no interior dos veículos, confrontando-as com os registros biométricos previamente cadastrados pelos beneficiários. Identificada eventual incompatibilidade, procede-se à inspeção visual para constatação do uso indevido do benefício, com posterior encaminhamento dos resultados à entidade gestora do sistema para apuração administrativa, assegurados o contraditório e a ampla defesa[21].

Embora implementada antes da vigência da LGPD, a política de reconhecimento biométrico no serviço de transporte submete-se às atuais normas de proteção de dados, visto que o tratamento ocorre continuamente. Nesse contexto, a hipótese fundamenta-se execução de políticas públicas[22], o que afasta a necessidade de consentimento, o que não se confunde com a inobservância dos princípios ínsitos ao tratamento, como finalidade, adequação, necessidade e segurança.

Nesse ponto, observa-se que a finalidade pública da implementação tecnológica não impediu o redirecionamento dos encargos de custeio, estruturação e operacionalização do sistema biométrico ao delegatário[23]. Na prática, tal configuração transfere o armazenamento e a custódia direta desses ativos informacionais sensíveis à esfera de entes privados, ainda que sob a tutela estatal. Essa descentralização administrativa potencializa a vulnerabilidade dos dados biométricos, especialmente ante a carência de diretrizes técnicas rigorosas de segurança, como criptografia, anonimização ou protocolos de retenção temporal, essenciais para mitigar eventuais incidentes.

Salienta-se que, em buscas realizadas em fontes públicas disponíveis on-line, não se verificou a existência do Relatório de Impacto à Proteção de Dados (RIPD) referente a essa política, o que dificulta a análise aprofundada das circunstâncias que envolvem o tratamento, bem como a aferição objetiva da necessidade, da proporcionalidade e das salvaguardas efetivamente implementadas no processamento dos dados biométricos faciais dos usuários.

Apesar disso, as portarias sobre o tema[24], evidenciam que a política pública de reconhecimento facial no transporte coletivo concentrou-se no combate a fraudes no uso do benefício, sem demonstração concreta da efetividade da medida, tampouco do devido sopesamento dos impactos sobre as liberdades individuais dos beneficiários.

Então, os titulares veem-se diante da seguinte ponderação: aceitar a exposição de seus dados biométricos faciais ou arcar com o custo da passagem. Logo, a atuação estatal corrobora a crítica formulada por Lyon, com esteio em Wacquant, acerca do panoptismo social, no qual a vigilância incide de forma especialmente rigorosa sobre grupos socialmente vulneráveis, a exemplo dos beneficiários de políticas assistenciais[25], sobretudo quando a escassez de elementos sólidos sobre a efetividade da medida não elimina tal pressuposição.

3.3. Caso das Escolas do Paraná

No Paraná, a implementação da biometria facial no ambiente escolar visou automatizar o controle de frequência na rede pública estadual. A iniciativa fundamentou-se na busca por eficiência administrativa, sobretudo na mitigação do tempo dedicado a tarefas burocráticas: estima-se que o registro automatizado reduza o

período despendido pelo docente de uma média de 5 a 10 minutos para apenas 1 ou 2 minutos por aula, a depender da sua familiaridade com a tecnologia[26].

Como funciona? A cada aula, o professor registra imagens da turma por meio de aplicativo instalado em telefone celular, encaminhando-as para processamento automatizado. Inicialmente, realiza-se o cadastro biométrico do estudante com três fotografias, vinculadas ao seu registro escolar. Essas imagens são enviadas à Celepar[27] por protocolo seguro e armazenadas em servidor próprio, sem permanência no aparelho utilizado para a captura. Após o processamento pelo fornecedor responsável, é gerada uma chave de identificação (hash), posteriormente associada ao Código Geral de Matrícula (CGM) do aluno[28].

Considerando que a iniciativa foi estruturada já sob a vigência da LGPD, a Secretaria de Estado da Educação e do Esporte do Paraná elaborou Relatório de Impacto à Proteção de Dados Pessoais (RIPD) específico para o projeto de reconhecimento facial destinado ao registro de frequência escolar[29]. Nele, o tratamento é justificado pelo cumprimento de obrigação legal relacionada ao controle de frequência e pela execução de política pública educacional, afastando, assim, a exigência de consentimento como base legal principal.

Contudo, o documento revela inconsistências analítica, como a previsão dos princípios expressos da LGPD como meras recomendações de boas práticas, despojando-os de sua natureza de deveres cogentes inerentes a qualquer tratamento de dados. E, embora sustente a observância do princípio da necessidade pelo uso

do mínimo de dados possível para a implementação da tecnologia, essa análise mostra-se insuficiente.

O princípio da necessidade não se limita à redução quantitativa de dados coletados, exigindo a verificação da indispensabilidade do próprio tratamento, à luz da proporcionalidade e da existência de meios menos invasivos para atingir a mesma finalidade. Além disso, o RIPD não enfrentou de forma adequada os índices de falhas na identificação algorítmica nem apresentou mecanismos efetivos de controle e limitação do tratamento de dados dos estudantes, que permanecem submetidos a sucessivos reconhecimentos faciais no cotidiano escolar.

Diante disto, em 2025, a 3ª Promotoria de Justiça de Campo Mourão ajuizou Ação Civil Pública em face do Estado do Paraná, da Celepar e da empresa privada responsável pela operação do sistema, questionando a legalidade da coleta de biometria facial de estudantes para controle de presença escolar.

Alega-se violação à LGPD sob quatro fundamentos principais: afronta aos princípios previstos no art. 6º; violação ao direito à autodeterminação informativa; tratamento de dados pessoais sem adequada sustentação em bases legais válidas; e invalidade do consentimento fornecido pelos pais ou responsáveis legais dos estudantes[30]. Tais pontos sintetizam as principais inconsistências da política estatal.

Os casos apresentados revelam um panorama de implementação da biometria facial pautado, primordialmente, por critérios de eficiência operacional e segurança. Observa-se, contudo, a carência de uma análise prévia e detalhada sobre os riscos à proteção de

dados, o que compromete severamente as liberdades individuais dos titulares, sobretudo daqueles em maior condição de vulnerabilidade.

4. PARÂMETROS JURÍDICOS DE CONTROLE DA BIOMETRIA FACIAL

A elevação da proteção de dados pessoais à condição de direito fundamental, promovida pela Emenda Constitucional n. 115/2022, reforça a centralidade do tema e impõe sua interpretação sistemática com os demais direitos fundamentais e a estrutura infraconstitucional já existente[31].

Nesse contexto, a utilização de dados biométricos faciais pela Administração Pública deve observar rigorosamente os princípios da LGPD, com ênfase no princípio da necessidade[32], que impõe a limitação do tratamento ao mínimo indispensável para o cumprimento de sua finalidade, exigindo a utilização apenas de dados pertinentes, proporcionais e não excessivos.

De modo similar, o Regulamento Geral de Proteção de Dados da União Europeia dispõe que os dados pessoais devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados, consagrando a lógica de minimização como elemento estruturante do tratamento (art. 5º, n. 1, alínea c, do GDPR).

Considerando as previsões normativas, sustenta-se a utilização do princípio da necessidade como filtro material e prévio ao tratamento, de modo que a licitude do uso de dados biométricos faciais depende da demonstração concreta de sua

indispensabilidade para o atendimento de finalidade específica, não se admitindo sua adoção por mera conveniência.

Tendo em vista a implementação prática desse filtro material da necessidade, o RIPD apresenta-se como instrumento prévio e obrigatório para a utilização de dados pessoais sensíveis, especialmente diante dos potenciais riscos às liberdades civis e aos direitos fundamentais[33]. Nesse relatório, devem ser demonstrados os pressupostos de legitimidade do tratamento, dentre os quais se destacam a finalidade[34], a adequação[35] e a própria necessidade, particularmente relevantes na atuação administrativa em razão da prevalência do interesse público primário.

Tal cautela justifica-se, sobretudo, pelas situações narradas no capítulo anterior, as quais demonstram uma atuação estatal frequentemente exercida em parceria com o setor privado. Nesses casos, a fundamentação genérica no cumprimento de dever legal ou execução de políticas públicas é insuficiente: o compartilhamento de dados biométricos com entes privados exige observância estrita aos princípios da LGPD e a instituição de mecanismos efetivos de proteção, sobretudo diante da natureza imutável do dado biométrico facial.

Somado a isso, a institucionalização dessa limitação prévia contribui para reduzir a sobrecarga decisória imposta ao titular[36]. Simultaneamente, tal medida reforça os deveres de conformidade (*compliance*) e de prestação de contas (*accountability*) do agente de tratamento — seja ele público ou privado —, assegurando que apenas operações de tratamento efetivamente indispensáveis sejam executadas.

A aplicação prática dessas balizas revela-se nítida no caso do Metrô de São Paulo, uma vez que a extração de dados sensíveis, como sexo, idade e origem racial por meio da biometria facial, para fins publicitários, revela-se desproporcional e dissociada da finalidade essencial do serviço público, especialmente diante da existência de métodos estatísticos menos invasivos.

No que tange à implementação da biometria no sistema de bilhetagem do Distrito Federal, embora o combate a fraudes no transporte público represente um objetivo legítimo, a conformidade com a LGPD resta comprometida pela ausência de demonstração técnica sobre a indispensabilidade da medida. De mais a mais, a finalidade fiscalizatória poderia ser plenamente atingida por mecanismos menos intrusivos e já consolidados, a exemplo de cartões personalizados com fotografia, fiscalização presencial ou auditorias por amostragem, o que evidencia o excesso no tratamento desses dados biométricos.

Por fim, no caso das escolas do Paraná, a necessidade da medida não restou evidenciada, especialmente quando confrontada com o elevado dispêndio de recursos públicos em face do benefício administrativo pretendido. Além disso, o tratamento de dados de crianças e adolescentes exige rigor protetivo acentuado, devendo pautar-se pelo princípio do melhor interesse, diretriz que não se verificou no Relatório de Impacto à Proteção de Dados Pessoais (RIPD) apresentado.

É pertinente mencionar, nesse sentido, o precedente sueco, no qual um conselho escolar foi multado por implementar sistema análogo. Naquela oportunidade, o regulador europeu enfatizou que o desequilíbrio de força entre a instituição e os alunos impede que

estes consintam livremente com tecnologias de vigilância em sala de aula; ademais, destacou que a frequência escolar pode ser monitorada por métodos menos gravosos à integridade dos estudantes[37].

De todo o exposto, reitera-se que a inovação tecnológica na Administração Pública deve permanecer subordinada ao interesse público primário e à salvaguarda dos direitos fundamentais, evitando que se converta em fundamento autônomo para a expansão de mecanismos de controle. A proteção de dados pessoais sensíveis, notadamente em matéria biométrica, exige que a excepcionalidade do tratamento seja cabalmente comprovada, e não meramente presumida, garantindo que a busca por eficiência não comprometa a dignidade, a privacidade e a autodeterminação informativa dos titulares.

5. CONCLUSÃO

De acordo com Colombo e Goulart[38], os dados biométricos ocupam posição singular no regime de proteção de dados pessoais, pois estão diretamente vinculados às características corporais do titular e apresentam elevado potencial identificador, muitas vezes próximo da identificabilidade absoluta. Sendo assim, a naturalização de seu uso em situações cotidianas e substituíveis por meios menos invasivos revela uma banalização preocupante do tratamento biométrico, incompatível com a lógica da necessidade e da minimização de dados.

Ao longo deste estudo, evidenciou-se que o emprego da biometria facial pela Administração Pública tem sido legitimado pela eficiência, segurança e modernização. Todavia, a prática demonstra

que tal implementação ocorre, frequentemente, à revelia de uma comprovação técnica sobre a sua indispensabilidade. A confirmação da hipótese central é, portanto, nítida: ao migrar de contextos excepcionais para atividades ordinárias (como o controle de frequência escolar e a fiscalização de gratuidades), o tratamento de dados sensíveis passa a integrar rotinas administrativas sem a devida observância dos limites impostos pela LGPD e pela Constituição Federal.

Essa onipresença tecnológica não é inócua. Falhas sistêmicas, como falsos positivos, podem produzir danos de difícil reparação, restringindo direitos sociais básicos ou interferindo nas liberdades individuais. A prisão ilegal de Silvio Gabriel Juarez[39], que, em 2024, foi erroneamente identificado como autor de um furto ocorrido em 2020, ilustra o risco de se confiar cegamente em decisões automatizadas. Ademais, a persistência dessa banalização tende a ampliar não apenas os danos individuais e coletivos, mas também a própria responsabilidade objetiva do Estado (art. 37, § 6º, CF), onerando a Administração pelo dever de reparar prejuízos causados por seus agentes e sistemas.

Diante desse cenário, conclui-se que o princípio da necessidade deve atuar como um critério material de contenção: um filtro prévio de legitimidade, e não meramente uma etapa posterior de mitigação de danos. Cabendo à Administração Pública o ônus de demonstrar, de forma objetiva, que a coleta da biometria facial é indispensável e que inexistem meios menos invasivos para alcançar o mesmo resultado.

Em última análise, a inovação tecnológica deve permanecer subordinada à dignidade humana e à autodeterminação

informativa. Proteger dados biométricos exige resgatar o caráter excepcional de seu tratamento, impedindo que o corpo do indivíduo seja reduzido a um instrumento permanente de vigilância e que o "cotidiano" administrativo se sobreponha aos direitos fundamentais.

REFERÊNCIAS BIBLIOGRÁFICAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS – ANPD. **Radar tecnológico nº 2:** biometria e reconhecimento facial – estudos preliminares. Coord. Fabiana S. P. Faraco Cebrian et al. Brasília: ANPD, jun. 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-biometria-anpd-1. Acesso em: 05 maio 2025.

BRASIL. **Decreto nº 10.977, de 23 de fevereiro de 2022.** Regulamenta a Lei nº 7.116, de 29 de agosto de 1983, para estabelecer os procedimentos e os requisitos para a expedição da Carteira de Identidade por órgãos de identificação dos Estados e do Distrito Federal, e a Lei nº 9.454, de 7 de abril de 1997, para estabelecer o Serviço de Identificação do Cidadão como o Sistema Nacional de Registro de Identificação Civil. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/d10977.htm. Acesso em: 25 abr. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 7 maio 2025.

BRASIL. **Lei nº 13.444, de 11 de maio de 2017.** Dispõe sobre a Identificação Civil Nacional (ICN). Brasília, DF: Presidência da

República, 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13444.htm. Acesso em: 25 abr. 2026.

BRASIL. Tribunal Superior Eleitoral. **Resolução n.º 22.688, de 13 de dezembro de 2007.** Disciplina os procedimentos para a atualização do cadastro eleitoral, decorrente da implantação, em caráter experimental, de nova sistemática de identificação do eleitor, mediante incorporação de dados biométricos e fotografia. Brasília, DF: Tribunal Superior Eleitoral, 2007. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2007/resolucao-no-22-688-de-13-de-dezembro-de-2007. Acesso em: 10 fev. 2026

BAUMAN, Zygmunt; LYON, David. **Vigilância líquida.** Tradução autorizada da 1ª edição inglesa publicada em 2013 por Polity Press. Rio de Janeiro: Zahar, 2014. E-book (edição Kindle).

CNN BRASIL. **Veja esquema especial de segurança do Governo do Rio para show de Lady Gaga.** CNN Brasil, São Paulo, 3 maio 2025. Disponível em: https://www.cnnbrasil.com.br/nacional/sudeste/rj/veja-esquema-especial-de-seguranca-do-governo-do-rio-para-show-de-lady-gaga/. Acesso em: 07 maio 2025. Acesso em: 07 maio 2025

COLOMBO, Cristiano; GOULART, Guilherme Damasio. **Novo perímetro do corpo e a biometria como dado pessoal:** princípios da finalidade e da necessidade aplicados e recomendações para o caso do metrô de São Paulo. In: COLOMBO, Cristiano; ENGELMANN, Wilson; FALEIROS JÚNIOR, José Luiz de Moura (coord.). Tutela jurídica do corpo eletrônico: novos desafios ao direito digital. 1. ed. Indaiatuba, SP: Editora Foco, 2022.

COMPANHIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO PARANÁ (CELEPAR). **Apresentação.** Curitiba, [s.d.]. Disponível em: https://www.celepar.pr.gov.br/Pagina/Apresentacao. Acesso em: 24 abr. 2026.

DISTRITO FEDERAL. Secretaria de Estado de Transporte e Mobilidade. **Perguntas frequentes da SEMO**B. Brasília, 15 fev. 2025. Atualizado em: abr. 2026. Disponível em: https://www.semob.df.gov.br/perguntas-frequentes-da-semob. Acesso em: 17 abr. 2026.

DISTRITO FEDERAL. Departamento de Trânsito do Distrito Federal (DFTRANS). **Portaria n. 15, de 30 de abril de 2018.** Dispõe sobre a utilização do controle biométrico facial no Sistema de Bilhetagem Automática do Sistema de Transporte Público Coletivo do Distrito Federal – STPC/DF. Diário Oficial do Distrito Federal, Brasília, DF, 2 maio 2018. Disponível em: https://www.sinj.df.gov.br/sinj/Norma/39e7cf5acaba49a4a381f9dc2d74e92d/Portaria_15_30_04_2018.html. Acesso em: 23 abr. 2026.

DISTRITO FEDERAL. Secretaria de Estado de Mobilidade. **Portaria n. 11, de 28 de março de 2018.** Torna obrigatória a utilização de biometria facial como forma de combate às fraudes no uso de gratuidades tarifárias e no vale-transporte do Sistema de Transporte Público Coletivo do Distrito Federal – STPC/DF. Diário Oficial do Distrito Federal, Brasília, DF, n. 62, seção 1, 2 e 3, p. 15, 2 abr. 2018. Disponível em: https://www.sinj.df.gov.br/sinj/Norma/8540909caaae4ac9895dc39625683915/Portaria_11_28_03_2018.html. Acesso em: 24 abr. 2026.

FELICIANO, Guilherme Guimarães; NASPOLINI, Samyra Haydêe Dal Farra; FOGAROLLI FILHO, Paulo Roberto. **O capitalismo de vigilância e seus efeitos:** discriminação algorítmica e reificação humana. Revista de Direito Brasileira, v. 33, n. 12, p. 309-330, set. 2023. DOI: 10.26668/IndexLawJournals/2358-1352/2022.v33i12.9167.

ILLINOIS (State). **Biometric Information Privacy Act. 740 ILCS 14/.** Illinois Compiled Statutes. Springfield: Illinois General Assembly, 2008. Disponível em: https://www.ilga.gov/Legislation/ILCS/Articles?ActID=3004&ChapterID=57&Print=True. Acesso em: 19 fev. 2026.

INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS. **INSS inicia projeto piloto de prova de vida digital. Brasília:** INSS, 20 jan. 2021. Disponível em: https://www.gov.br/inss/pt-br/noticias/noticias/inss-inicia-projeto-piloto-de-prova-de-vida-digital. Acesso em: 07 maio 2025

MINISTÉRIO PÚBLICO DO ESTADO DO PARANÁ (MPPR). **Promotoria de Justiça em Campo Mourão ajuíza ação civil por violação à Lei Geral de Proteção de Dados na coleta de biometria facial** de alunos de escolas públicas. Curitiba, 28 abr. 2025. Disponível em: https://mppr.mp.br/Noticia/Promotoria-de-Justica-em-Campo-Mourao-ajuiza-acao-civil-por-violacao-Lei-Geral-de-Protecao. Acesso em: 20 abr. 2026.

MOREIRA, Ana Flávia Sales; MOREIRA, Andréa Cristiane Sales; MOREIRA, Clarisse Sales. **Aspectos da privacidade na sociedade de vigilância:** proteção de dados e sistemas de videomonitoramento. Revista da EMERJ, Rio de Janeiro, v. 26, e589, p. 1-23, 2024. Submissão em: 07 fev. 2024. Aprovação em: 25 jul. 2024 e 27 nov. 2024. Editor: Antonio Aurélio Abi Ramia. Disponível em:

https://ojs.emerj.com.br/index.php/revistadaemerj/article/view/589/338. Acesso em: 22 maio 2025.

NUNES, Pablo et al. **Mapeando a vigilância biométrica [livro eletrônico**]: levantamento nacional sobre o uso do reconhecimento facial na segurança pública. Rio de Janeiro: CESeC, 2025.Formato: PDF. 2,5 MB. ISBN: 978-85-5969-057-6. Disponível em: https://drive.google.com/file/d/1bN2ssBp_dMiih8YOUonLhGl_5jRoNe5s/view. Acesso em: 07 maio 2025

PARANÁ. Secretaria de Estado da Educação e do Esporte. **Relatório de impacto à proteção de dados pessoais:** projeto reconhecimento facial. Curitiba, 25 jan. 2021. Disponível em: https://www.educacao.pr.gov.br/sites/default/arquivos_restritos/files/documento/2024-07/ripd_pr_v1_6_reconhecimento_facial_prot172811760.pdf. Acesso em: 24 abr. 2026

PASQUALE, Frank. **The Black Box Society:** The Secret Algorithms That Control Money and Information. Cambridge, Massachusetts: Harvard University Press, 2015. Disponível em: https://tetrazolelover.at.ua/Frank_Pasquale-The_Black_Box_Society-The_Secret_Al.pdf. Acesso em: 20 out. 2025

SARLET, Ingo Wolfgang. **A EC 115/22 e a proteção de dados pessoais como direito fundamental** I. Consultor Jurídico, 11 mar. 2022. Disponível em: https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental/. Acesso em: 20 abr. 2026.

SCHMIDT, Nico; COELHO, Leonardo; NÚCLEO JORNALISMO. **Sistema de reconhecimento facial monitora alunos no Brasil.** Agência

Pública, 18 mar. 2026. Disponível em: https://apublica.org/2026/03/reconhecimento-facial-sistema-monitora-alunos-no-brasil/. Acesso em: 20 abr. 2026.

SOUZA, Felipe Gabriades de. **O mito da supremacia do consentimento:** o mecanismo de pluralidade de bases legais da LGPD. 2024. 84 f. Dissertação (Mestrado Profissional em Direito) – Escola de Direito de São Paulo, Fundação Getulio Vargas, São Paulo, 2024.

UNIÃO EUROPEIA. **Grupo de Trabalho do Artigo 29.º**. Parecer n. 3/2012 sobre a evolução das tecnologias biométricas. Bruxelas, 27 abr. 2012. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_pt.pdf. Acesso em: 15 jan. 2026.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, L 119, p. 1–88, 04 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX%3A32016R0679. Acesso em: 03 maio 2025.

Autora 1- Mestranda em Direito Constitucional Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP). Pesquisadora do Grupo de Pesquisa Responsabilidade Civil e Perspectiva Comparada (RCPC). Advogada.

[1] FELICIANO; NASPOLINI; FOGAROLLI FILHO, 2023, p. 3-4

[2] BRASIL. Tribunal Superior Eleitoral. Resolução n.º 22.688, de 13 de dezembro de 2007. Disciplina os procedimentos para a atualização do cadastro eleitoral, decorrente da implantação, em caráter experimental, de nova sistemática de identificação do eleitor, mediante incorporação de dados biométricos e fotografia. Brasília, DF: Tribunal Superior Eleitoral, 2007. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2007/resolucao-no-22-688-de-13-de-dezembro-de-2007. Acesso em: 10 fev. 2026

[3] NUNES, Pablo et al. Mapeando a vigilância biométrica [livro eletrônico]: levantamento nacional sobre o uso do reconhecimento facial na segurança pública. Rio de Janeiro: CESeC, 2025.Formato: PDF. 2,5 MB. ISBN: 978-85-5969-057-6. Disponível em: https://drive.google.com/file/d/1bN2ssBp_dMiih8YOUonLhGl_5jRoNe5s/view. Acesso em: 7 maio 2025

[4] *Ibid.*

[5] CNN BRASIL. Veja esquema especial de segurança do Governo do Rio para show de Lady Gaga. CNN Brasil, São Paulo, 3 maio 2025. Disponível em: https://www.cnnbrasil.com.br/nacional/sudeste/rj/veja-esquema-especial-de-seguranca-do-governo-do-rio-para-show-de-lady-gaga/. Acesso em: 07 maio 2025

[6] Lei nº 13.444/

[7] INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS. INSS inicia projeto piloto de prova de vida digital. Brasília: INSS, 20 jan. 2021. Disponível em: https://www.gov.br/inss/pt-br/noticias/noticias/inss-

inicia-projeto-piloto-de-prova-de-vida-digital. Acesso em: 7 maio 2025

[8] Decreto nº 10.977/2

[9] Art. 5º, II, da Lei 13.709/2018.

[10] ANPD, 2024, p. 6 e 12.

[11] 740 ILCS 14/10 (Biometric Information Privacy Act, Illinois, 2008).

[12] Regulamento (UE) 2016/679.

[13] Emotion AI (ou Inteligência Artificial Emocional) consiste, tecnicamente, em "um sistema de IA concebido para identificar ou inferir emoções ou intenções de pessoas singulares com base nos seus dados biométricos" (Regulamento (UE) 2024/1689, art. 3.º, n.º 39).

[14] ANPD, 2024, p. 12.

[15] GT29, 2012, p. 21.

[16] A decisão não é definitiva. Em 23 de abril de 2025, o processo foi encaminhado ao Superior Tribunal de Justiça (STJ), onde aguarda julgamento do recurso interposto pela concessionária. Fonte: SÃO PAULO. Tribunal de Justiça. Apelação Cível nº 1090663-42.2018.8.26.0100. Movimentação de 23 abr. 2025. Disponível em: esaj.tjsp.jus.br. Acesso em: 21 nov. 2025.

[17] MOREIRA; MOREIRA; MOREIRA, 2024, p. 14.

[18] A Lei nº 13.709/2018 (LGPD) teve vigência fragmentada: os artigos relativos à criação da ANPD entraram em vigor em 28/12/2018; os dispositivos sobre direitos e obrigações (corpo principal) em 18/09/2020; e as sanções administrativas (arts. 52-54) apenas em 01/08/2021, por força da Lei nº 14.010/2020. No Caso ViaQuatro, os fatos (abril/2018) precederam a vigência, motivando o uso da LGPD como reforço hermenêutico às garantias já previstas no CDC e na CF/88.

[19] O caso ViaQuatro também é anterior à promulgação da Emenda Constitucional n. 115/2022, que elevou expressamente a proteção de dados pessoais à categoria de direito fundamental, mediante inclusão do inciso LXXIX ao art. 5º da Constituição Federal. Sendo assim, a base constitucional expressamente mobilizada na sentença estava relacionada a outros direitos fundamentais, como à intimidade, à privacidade, à imagem e à honra.

[20] PASQUALE, 2015, p. 10.

[21] DISTRITO FEDERAL. Secretaria de Estado de Transporte e Mobilidade. Perguntas frequentes da SEMOB. Brasília, 15 fev. 2025. Atualizado em: abr. 2026. Disponível em: https://www.semob.df.gov.br/perguntas-frequentes-da-semob. Acesso em: 17 abr. 2026.

[22] Art. 7º, III, da Lei n. 13.709/2018.

[23] DFTRANS, Portaria nº 15/2018.

[24] DFTRANS, Portarias n. 11 e 15/2018.

[25] BAUMAN; LYON, 2014, p. 51

[26] PARANÁ, 2021, p. 7.

[27] A Celepar – Companhia de Tecnologia da Informação e Comunicação do Paraná, é uma sociedade de economia mista do Governo do Estado do Paraná, fundada em 1964.

[28] PARANÁ, 2021, p. 5.

[29] PARANÁ. Secretaria de Estado da Educação e do Esporte. Relatório de impacto à proteção de dados pessoais: projeto reconhecimento facial. Curitiba, 25 jan. 2021. Disponível em: https://www.educacao.pr.gov.br/sites/default/arquivos_restritos/files/documento/2024-07/ripd_pr_v1_6_reconhecimento_facial_prot172811760.pdf. Acesso em: 24 abr. 2026.

[30] A demanda tramita perante a 1ª Vara da Fazenda Pública de Campo Mourão, sob o processo 0004208-55.2025.8.16.0058, sem sentença até o momento.

[31] SARLET, Ingo Wolfgang. A EC 115/22 e a proteção de dados pessoais como direito fundamental I. Consultor Jurídico, 11 mar. 2022. Disponível em: https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental/. Acesso em: 20 abr. 2026

[32] Art. 6°, III, da Lei 13.709/2018.

[33] Art. 5°, XVII, da Lei 13.709/2018.

[34] Art. 6º, I, da Lei 13.709/2018.

[35] Art. 6º, II, da Lei 13.709/2018.

[36] SOUZA, 2024, p. 63-64.

[37] SCHMIDT, Nico; COELHO, Leonardo; NÚCLEO JORNALISMO. Sistema de reconhecimento facial monitora alunos no Brasil. Agência Pública, 18 mar. 2026. Disponível em: https://apublica.org/2026/03/reconhecimento-facial-sistema-monitora-alunos-no-brasil/. Acesso em: 20 abr. 2026.

[38] COLOMBO; GOULART, 2022, p. 815 e 817.

[39] GRINBERG; ARAÚJO; FREITAS; RIBEIRO, 2024.