Revista da Faculdade de Direito do Sul de Minas
ISSN 1516-4551 • ISSN-e 2447-8709

CÂMERAS NA ESCOLA: VIGILÂNCIA, DIREITOS FUNDAMENTAIS E A REGULAÇÃO MUNICIPAL EM CAMPINAS, SÃO PAULO E SÃO JOSÉ DO RIO PRETO

CAMERAS IN SCHOOLS: SURVEILLANCE, FUNDAMENTAL RIGHTS AND MUNICIPAL REGULATION IN CAMPINAS, SÃO PAULO AND SÃO JOSÉ DO RIO PRETO

Lucas Catib de Laurentiis [*]
Vitória Cecchi Costa [**]
Arnaldo de Santana Silva [***]

RESUMO

Desde 2018, e com mais intensidade após a onda de ataques a escolas de 2023, municípios paulistas passaram a instalar câmeras nas unidades de ensino e a regular seu uso. O artigo compara três modelos dessa regulação: o decreto de Campinas que disciplina as câmeras do Protocolo Égide; a portaria conjunta das secretarias de Educação e de Segurança Urbana de São Paulo, que integra as escolas municipais ao Programa Smart Sampa; e a lei de São José do Rio Preto, que impôs câmeras em creches e escolas, inclusive em salas de aula, e foi mantida pelo Tribunal de Justiça de São Paulo. O método é a análise documental comparada das normas e da decisão judicial, com parâmetros extraídos da literatura sobre vigilância, videomonitoramento e reconhecimento facial e do regime de proteção de dados de crianças. O artigo sustenta que os três municípios regularam o funcionamento das câmeras e deixaram sem resposta a questão que deveria anteceder a instalação: qual risco concreto justifica vigiar a escola, com que prova de que a medida o reduz e com que limites ao uso dos dados coletados. Os modelos diferem no grau em que incorporam a escola ao aparato de segurança urbana, e essa incorporação desloca a escola do campo da proteção integral da criança para o campo da segurança pública. Conclui-se que a regulação deve condicionar cada instalação a justificativa concreta e relatório de impacto, excluir sem exceção os espaços de ensino e de intimidade, proibir o reconhecimento facial e submeter o sistema a controle independente da área de segurança.

Palavras-chave: vigilância; videomonitoramento; reconhecimento facial; violência escolar; proteção de dados de crianças.

ABSTRACT

Since 2018, and more intensively after the wave of school attacks in 2023, municipalities in the state of São Paulo began installing cameras in schools and regulating their use. The article compares three regulatory models: the Campinas

[*] Doutor e mestre em Direito Constitucional pela Universidade de São Paulo (USP), especialista em Direito Constitucional pela Pontifícia Universidade Católica de São Paulo (PUC-SP), graduado em Direito pela PUC-SP e em Filosofia pela USP. É professor permanente do Programa de Pós-Graduação em Comunicação da Universidade Estadual Paulista (Unesp) e professor da Faculdade de Direito de São Bernardo do Campo. É também pesquisador vinculado à Escola de Direito de São Paulo da Fundação Getulio Vargas (FGV Direito SP) e à Universidade Estadual de Campinas (Unicamp). Lattes: http://lattes.cnpq.br/2294492760875997. Orcid: https://orcid.org/0000-0001-5596-6695.

[**] Graduada em Direito pela Pontifícia Universidade Católica de Campinas (PUC-Campinas), onde desenvolveu pesquisa de iniciação científica em Cooperação Internacional e Direitos Humanos, sob orientação do Prof. Dr. Lucas Catib De Laurentiis. Lattes: http://lattes.cnpq.br/5609752159090202.

[***] Mestre em Relações Internacionais pela UFABC, especialista em Direitos Humanos e Contemporaneidades pela UFBA e em Educação em Direitos Humanos pela UFABC, graduado em Relações Internacionais pela UNILAB e em Direito pela Universidade Católica do Salvador. É advogado, presidente da Comissão de Diversidade Sexual e Gênero da OAB de São Bernardo do Campo, pesquisador da organização ReportOUT e integrante da organização do Youth LACIGF. Lattes: http://lattes.cnpq.br/8934413288544663. Orcid: https://orcid.org/0000-0003-0333-6901.

Open Access. Double Blind Review pelo SEER/OJS.

Licença Creative Commons 3.0

decree governing the cameras of the Égide Protocol; the joint ordinance of the São Paulo Municipal Secretariats of Education and Urban Security, which integrates municipal schools into the Smart Sampa program; and the São José do Rio Preto law, which required cameras in daycare centers and schools, classrooms included, and was upheld by the São Paulo State Court of Justice. The method is a comparative documentary analysis of the regulations and the court decision, using parameters drawn from the literature on surveillance, video monitoring, and facial recognition, as well as the legal framework for protecting children's data. The article argues that the three municipalities regulated how the cameras operate and left unanswered the question that should precede their installation: which concrete risk justifies watching the school, what evidence shows that the measure reduces it, and which limits apply to the use of the data collected. The models differ in how far they incorporate the school into the urban security apparatus, and this incorporation moves the school from the field of children's integral protection to the field of public security. It concludes that regulation should make each installation conditional on concrete justification and an impact assessment, exclude teaching and intimate spaces without exception, prohibit facial recognition, and subject the system to oversight independent of the security authorities.

Key-words: surveillance; CCTV; facial recognition; school violence; children's data protection.

INTRODUÇÃO

Entre 2001 e 2024, o Brasil registrou 43 ataques a escolas, com 168 vítimas e 47 mortos, e a maior parte desses episódios concentrou-se em 2022 e 2023.[1] Os ataques de março e abril de 2023, em São Paulo e Blumenau, provocaram uma resposta pública rápida e de natureza securitária. Nesse contexto, governos estaduais e municipais anunciaram rondas policiais, monitoramento de redes sociais, protocolos de resposta a incidentes e, sobretudo, a instalação de câmeras nas escolas. A implantação de câmeras tornou-se a medida mais visível dessa resposta. Sua instalação, entretanto, cria um sistema permanente de coleta de imagens de crianças, adolescentes, professores e funcionários. Câmeras ligadas a centrais municipais de monitoramento e, em alguns casos, a programas que utilizam reconhecimento facial, aproximam o cotidiano escolar das técnicas empregadas para vigiar ruas, estações e fronteiras. Nos casos examinados, a regulação desse uso coube aos municípios, que o disciplinaram por lei, decreto ou portaria, sem parâmetro nacional específico.

O artigo compara três modelos de regulação municipal de câmeras em escolas no estado de São Paulo. O primeiro é o Decreto nº 24.328, de 5 de março de 2026, de Campinas, que estabelece princípios e parâmetros para as câmeras do Protocolo Égide. O segundo é a Portaria Conjunta SME/SMSU nº 4, de 12 de dezembro de 2024, do município de São Paulo, que integra as escolas municipais ao Programa "Smart Sampa". O terceiro é a Lei nº 12.953/2018, do município de São José do Rio Preto, que tornou obrigatória a instalação de câmeras em creches e escolas públicas municipais, inclusive em salas de aula, e teve sua validade confirmada pelo Órgão Especial do Tribunal de Justiça de São Paulo.

Sustentamos que os três municípios regularam o funcionamento das câmeras e deixaram sem resposta a pergunta que deveria ter precedido a instalação. As normas definem onde as câmeras podem ficar, quem pode ver as imagens e por quanto tempo elas são

[1] QUEIROZ, Christina. Disseminação de discursos de ódio agrava violência escolar. Revista Pesquisa FAPESP, São Paulo, n. 350, abr. 2025. Disponível em: https://revistapesquisa.fapesp.br/disseminacao-de-discursos-de-odio-agrava-violencia-escolar/. Acesso em: 18 out. 2026.

Licença *Creative Commons 3.0*

armazenadas, mas nenhuma delas exige que se demonstre qual risco concreto justifica vigiar uma escola determinada e em que medida a instalação das câmeras reduz esse risco. Os três modelos diferem no grau em que incorporam a escola ao aparato municipal de segurança urbana: Campinas espelha as imagens em tempo real para uma central de segurança, mas veda a instalação nos espaços de ensino; São Paulo insere as escolas em uma plataforma urbana de vigilância inteligente, que não prevê regras próprias para o ambiente escolar; São José do Rio Preto, enfim, leva a vigilância à sala de aula. Em todos esses casos, a escola passa a ser tratada como parte da rede de segurança pública, o que a afasta do regime de proteção integral que deveria orientar qualquer coleta de dados de crianças e adolescentes.

Para desenvolver esse argumento, o artigo segue cinco passos. A seção 2 trata a vigilância como problema jurídico. Ela mostra que a vigilância classifica pessoas e as seleciona para tratamento diferenciado, e que seus danos começam na coleta e na retenção dos dados, antes de qualquer exibição das imagens. Mostra também que esses danos atingem direitos além da privacidade e a própria confiança de que a escola depende. A seção 3 examina o que se sabe sobre a eficácia das câmeras e extrai da literatura os parâmetros para avaliá-las: justificativa concreta e prévia de cada instalação e exclusão de espaços de intimidade, de refúgio e de frequência reveladora de dados sensíveis. A seção 4 trata do reconhecimento facial, de seu uso na segurança pública e nas escolas brasileiras, e dos efeitos discriminatórios que ele produz sobre a população negra e estudantes pobres. As seções 5 e 6 analisam o decreto de Campinas, a inserção das escolas paulistanas no "Smart Sampa" e a lei de São José do Rio Preto mantida pelo Tribunal de Justiça. A seção 7 compara os três modelos à luz desses parâmetros e identifica os defeitos que eles compartilham. A conclusão indica o que uma regulação adequada deveria conter.

1 A VIGILÂNCIA COMO PROBLEMA JURÍDICO

1.1 Vigilância, classificação e poder

Uma definição de vigilância bastante aceita nos estudos sobre o tema a descreve como a atenção focada, sistemática e rotineira a detalhes pessoais, com fins de influência, gestão, proteção ou direção.[2] Essa atenção é, por vezes, realizada pelo Estado a partir da construção de políticas de segurança pública. A definição não depende da tecnologia empregada nem da intenção declarada de quem vigia. Câmeras instaladas para proteger alunos de um ataque também realizam a vigilância sistemática e rotineira de detalhes pessoais, e a finalidade de proteção convive com a capacidade de gerir e dirigir o comportamento de quem é observado.

Em termos sociais, as medidas de vigilância têm como traço central classificar as pessoas em grupos, convertendo dados pessoais em categorias de renda, atributos, hábitos, preferências ou infrações, com o fim de influenciá-las, geri-las ou controlá-las.[3] Aplicadas à gestão pública, essas classificações permitem tratar as pessoas de acordo com o lugar em que vivem ou com traços de seu corpo, e podem reproduzir estigmas no próprio tratamento dos dados. Essas categorias passam a influenciar as oportunidades de vida de pessoas e grupos. A gestão de riscos opera exatamente por essa via: ordena populações em categorias de risco para tratá-las de

[2] BERNAL, Paul. Data gathering, surveillance and human rights: recasting the debate. Journal of Cyber Policy, v. 1, n. 2, 2016, p. 249.
[3] HOROWITZ, Sarah. Foucault's Panopticon: a model for NSA surveillance? In: MILLER, Russell A. (ed.). Privacy and power: a transatlantic dialogue in the shadow of the NSA-Affair. Cambridge: Cambridge University Press, 2017, p. 52.

Licença *Creative Commons 3.0*

acordo com essas categorias.[4] Programas europeus de prevenção ao extremismo violento tendem a transformar a escola em espaço de detecção de indivíduos considerados em risco, o que converte a vigilância em um instrumento de seleção de estudantes suspeitos.[5]

Essa conversão foi descrita em outro contexto. Ao estudar práticas de municípios italianos em relação a migrantes, Enrico Gargiulo distinguiu a vigilância que monitora toda a população de um território daquela que categoriza e seleciona quem merece ser reconhecido como membro da comunidade.[6] No segundo caso, a vigilância deixa de produzir conhecimento sobre o conjunto dos vigiados e passa a separar os desejados dos indesejados. Com isso, a vigilância redefine as relações de poder e os arranjos institucionais.[7]

A mesma literatura critica a ideia de que a vigilância deva ser avaliada como uma troca entre segurança e privacidade. O modelo da troca é atraente pela simplicidade, porém opõe dois valores cujo significado é tomado como evidente, quando ambos são ambíguos e carregam sentidos muito diferentes.[8] Nesse sentido, no direito europeu, a privacidade funciona como um termo genérico que abrange direitos distintos, como o respeito à vida privada e a proteção de dados pessoais.[9] Por isso, a avaliação de uma medida de vigilância exige substituir os termos abstratos pelos direitos concretamente afetados e pelas medidas concretamente adotadas, além de tornar explícito o objetivo de segurança pretendido e a noção de risco que o sustenta.[10] O modelo da troca, por sua vez, faz com que o debate sobre liberdade e segurança pressuponha um jogo de soma zero, em que a segurança só se obtém à custa da liberdade.[11] Para a escola, isso significa que a pergunta sobre se a segurança dos alunos vale mais do que sua privacidade, que quase sempre favorece a câmera, deve dar lugar a outra: quais direitos de quais pessoas são atingidos pela coleta contínua de imagens, para enfrentar qual risco e com que evidência de que a medida o enfrenta.

1.2 Coleta, retenção e direitos além da privacidade

Paul Bernal distinguiu três momentos no processo de vigilância de dados: a coleta, a análise automatizada por algoritmos e o exame humano dos resultados. Governos que defendem programas de coleta massiva costumam afirmar que a vigilância só ocorre no terceiro momento, quando uma pessoa examina os dados. Bernal rejeita essa leitura e afirma que os principais riscos surgem na coleta de dados, pois a existência de dados já cria riscos de uso indevido, vazamento e desvio de finalidade. A jurisprudência europeia acompanha esse

[4] LYON, David. Surveillance, security and social sorting: emerging research priorities. International Criminal Justice Review, v. 17, n. 3, 2007, p. 162-163.
[5] MATTSSON, Christer; SÄLJÖ, Roger. Violent extremism, national security and prevention: institutional discourses and their implications for schooling. British Journal of Educational Studies, v. 66, n. 1, 2018, p. 110.
[6] GARGIULO, Enrico. Monitoring or selecting? Security in Italy between surveillance, identification and categorisation. In: ORRÙ, Elisa; PORCEDDA, Maria Grazia; WEYDNER-VOLKMANN, Sebastian (ed.). Rethinking surveillance and control: beyond the "security versus privacy" debate. Baden-Baden: Nomos, 2017, p. 206-207. No mesmo sentido, sobre a divisão binária entre perigosos e inofensivos e a vigilância mais intensa sobre os classificados como perigosos, HOROWITZ, Sarah. Foucault's Panopticon... 2017, p. 46.
[7] ORRÙ, Elisa; PORCEDDA, Maria Grazia; WEYDNER-VOLKMANN, Sebastian. Introduction. In: ORRÙ, Elisa; PORCEDDA, Maria Grazia; WEYDNER-VOLKMANN, Sebastian (ed.). Rethinking surveillance and control: beyond the "security versus privacy" debate. Baden-Baden: Nomos, 2017, p. 19.
[8] ORRÙ, Elisa; PORCEDDA, Maria Grazia; WEYDNER-VOLKMANN, Sebastian. Introduction... 2017, p. 17-18. No mesmo sentido, BERNAL, Paul. Data gathering, surveillance and human rights... 2016, p. 244.
[9] PORCEDDA, Maria Grazia. The recrudescence of 'security v. privacy' after the 2015 terrorist attacks, and the value of 'privacy rights' in the European Union. In: ORRÙ, Elisa; PORCEDDA, Maria Grazia; WEYDNER-VOLKMANN, Sebastian (ed.). Rethinking surveillance and control: beyond the "security versus privacy" debate. Baden-Baden: Nomos, 2017, p. 144.
[10] ORRÙ, Elisa; PORCEDDA, Maria Grazia; WEYDNER-VOLKMANN, Sebastian. Introduction... 2017, p. 19.
[11] LYON, David. Surveillance, security and social sorting... 2007, p. 164.

Licença Creative Commons 3.0

entendimento, afirmando que a simples retenção de dados pessoais por autoridades públicas afeta a vida privada, independentemente do uso posterior.[12]

A distinção entre coleta e acesso é central para a análise das normas municipais. Uma regulação que concentra seus controles no acesso às imagens, definindo quem pode vê-las e em que hipóteses, deixa sem controle o momento em que o risco nasce. Sistemas de vigilância ainda estão sujeitos a uso indevido, à perda, à invasão e ao chamado desvio de função, em que um sistema criado para uma finalidade passa a servir a outras.[13] Uma rede de câmeras escolares conectada a uma central de segurança pode, com uma mudança de software ou de regulamento, passar a identificar rostos, controlar frequência ou rastrear deslocamentos.[14]

O dano causado pelos sistemas de vigilância não se limita à eventual intrusão no conteúdo protegido do direito à privacidade. A vigilância também afeta a liberdade de expressão, a liberdade de reunião e de associação e a proibição de discriminação, seja porque a privacidade funciona como condição para o exercício desses direitos, seja porque a vigilância os atinge de forma direta.[15] Pesquisas empíricas mostram que pessoas que sabem estar sendo observadas evitam temas, reduzem sua participação e tendem ao conformismo.[16] Por isso, a literatura acrescenta uma dimensão crítica aos sistemas de vigilância que vai além da ideia de privacidade, pois a simples existência da vigilância retira liberdade, já que alguém – em geral, uma autoridade estatal – passa a ter o poder de observar quando quiser.[17] A intervenção no conteúdo do direito existe na mera possibilidade de interferência, e a liberdade depende dos arranjos institucionais que limitam essa possibilidade.[18] Essa formulação desloca a análise das câmeras do uso efetivo das imagens para a estrutura de poder que a instalação cria, o que torna decisivo saber quem controla o sistema e com que limites.

Por fim, a vigilância pode prejudicar a própria segurança que pretende produzir. Medidas excessivas podem reduzir a confiança nas instituições e, com ela, a cooperação das pessoas com as autoridades. Em uma sociedade democrática, as pessoas são presumidas dignas de confiança e a coleta generalizada de dados aproxima o Estado da lógica dos regimes autoritários, em que o exercício da liberdade é transformado em uma razão para a suspeita.[19] Na escola, esse custo recai sobre a própria formação dos alunos. A educação depende de um espaço em que o estudante possa formar e testar suas ideias, expressar-se e desenvolver-se sem ser tratado como suspeito. A câmera comunica desconfiança aos alunos, e essa desconfiança pode produzir o comportamento que pretende prevenir. Mesmo a demanda por segurança que nasce do medo dos professores compromete a qualidade da interação educativa. A vigilância permanente habitua os estudantes a achar normal serem observados o tempo todo e reduz a

[12] BERNAL, Paul. Data gathering, surveillance and human rights... 2016, p. 249 e 251, com referência ao caso S. and Marper v. the United Kingdom.
[13] BERNAL, Paul. Data gathering, surveillance and human rights... 2016, p. 251 e 260-261; CITRON, Danielle Keats; SOLOVE, Daniel J. Privacy harms. [S. l.: s. n.], 2021. Manuscrito, p. 34-35.
[14] CITRON, Danielle Keats; SOLOVE, Daniel J. Privacy harms... 2021, p. 45.
[15] BERNAL, Paul. Data gathering, surveillance and human rights... 2016, p. 245 e 257.
[16] BERNAL, Paul. Data gathering, surveillance and human rights... 2016, p. 255. No mesmo sentido, HOROWITZ, Sarah. Foucault's Panopticon... 2017, p. 54-55; CITRON, Danielle Keats; SOLOVE, Daniel J. Privacy harms... 2021, p. 27.
[17] BERNAL, Paul. Data gathering, surveillance and human rights... 2016, p. 250.
[18] HERRON, Patrick. Beyond balance: targeted sanctions, security and republican freedom. In: ORRÙ, Elisa; PORCEDDA, Maria Grazia; WEYDNER-VOLKMANN, Sebastian (ed.). Rethinking surveillance and control: beyond the "security versus privacy" debate. Baden-Baden: Nomos, 2017, p. 30-31.
[19] BERNAL, Paul. Data gathering, surveillance and human rights... 2016, p. 252 e 259-260. No mesmo sentido, HOROWITZ, Sarah. Foucault's Panopticon... 2017, p. 56.

Licença Creative Commons 3.0

capacidade de questionar essa observação, que a escola, comprometida com a liberdade de aprender e de ensinar, deveria desenvolver.[20]

2 CÂMERAS DE VIGILÂNCIA: EFICÁCIA E LIMITES

2.1 Eficácia das câmeras

A justificativa criminológica da implantação de câmeras está ligada à prevenção situacional do crime. Se o potencial infrator souber que está sendo observado, perceberá a maior probabilidade de ser identificado como autor e, com isso, tenderá a desistir do curso de sua ação delitiva.[21] A expansão das câmeras insere-se, assim, no que Garland chamou de cultura do controle, caracterizada pelo uso de políticas de controle social voltadas à visibilidade contínua e abrangente.[22] Porém, a crença de que basta instalar câmeras para reduzir a criminalidade não encontra respaldo teórico ou empírico. A câmera não é uma barreira física. Ela não impede o acesso a um lugar nem torna uma pessoa mais difícil de agredir. Seus efeitos dependem de dois mecanismos, a dissuasão do infrator e a identificação dos autores, e os resultados de sua aplicação são mistos.[23]

A dissuasão depende de duas condições: que o infrator saiba da existência das câmeras e que avalie racionalmente que o risco de ser apanhado supera o ganho do crime. A primeira condição pode falhar. Em Glasgow, quinze meses após a instalação de 32 câmeras no centro da cidade, apenas 41% dos entrevistados sabiam de sua existência. A segunda condição é questionada quando o infrator não age de forma calculada, como ocorre sob o efeito de álcool ou de drogas. Isso pode ajudar a explicar por que as câmeras parecem mais eficazes contra crimes patrimoniais do que contra desordem e crimes violentos. Por isso mesmo, há pouca evidência de que reduzam de modo significativo as agressões. Mesmo quando a dissuasão funciona, os infratores podem levar a conduta para fora do alcance das câmeras ou mudar sua forma de agir: em um dos casos relatados, traficantes passaram a negociar diante das câmeras e a concluir a transação em outro local.[24]

A identificação dos autores só atua depois que o crime começou e depende de condições externas à câmera. A gravação só tem utilidade se a polícia responder a tempo aos incidentes observados e se o sistema de justiça levar adiante a responsabilização. Mesmo quando essas condições existem, o efeito tende a diminuir com o tempo, porque os infratores aprendem quais incidentes provocam resposta e com que rapidez. A eficácia da câmera passa, assim, a depender dos recursos locais de polícia e de justiça, e os avaliadores consideram a redução do crime pela identificação menos convincente do que a obtida pela prevenção.[25] Pelo mesmo motivo, sistemas monitorados em tempo real, que permitem acionar a polícia durante o incidente,

[20] TAYLOR, Emmeline. I spy with my little eye: the use of CCTV in schools and the impact on privacy. The Sociological Review, v. 58, n. 3, 2010, p. 401.
[21] AGUSTINA, José R.; GALDON CLAVELL, Gemma. The impact of CCTV on fundamental rights and crime prevention strategies: the case of the Catalan Control Commission of Video surveillance Devices. Computer Law & Security Review, v. 27, n. 2, 2011, p. 168-169.
[22] GARLAND, David. The culture of control: crime and social order in contemporary society. Oxford: Oxford University Press, 2001.
[23] AGUSTINA, José R.; GALDON CLAVELL, Gemma. The impact of CCTV on fundamental rights... 2011, p. 169; RATCLIFFE, Jerry H.; ROSENTHAL, Jessica M. Video surveillance of public places. 2. ed. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services, 2021. (Problem-Oriented Guides for Police. Response Guide Series, n. 4), p. 10 e 29.
[24] RATCLIFFE, Jerry H.; ROSENTHAL, Jessica M. Video surveillance of public places... 2021, p. 10, 14 e 23.
[25] RATCLIFFE, Jerry H.; ROSENTHAL, Jessica M. Video surveillance of public places... 2021, p. 11.

Licença Creative Commons 3.0

reduzem mais o crime do que sistemas que apenas gravam imagens para consulta posterior.[26] A identificação produz ainda um efeito que dificulta medir a eficácia das câmeras: ao revelar ocorrências que antes não chegavam à polícia, elas podem aumentar o número de crimes registrados sem que a criminalidade tenha aumentado.[27] Por essas razões, os próprios avaliadores advertem que a câmera não serve para todas as circunstâncias e que uma medida dirigida ao problema específico pode bastar.[28]

Essas conclusões têm implicações para as políticas de vigilância implementadas nas escolas. Pesquisa nacional realizada no fim dos anos 1990 não encontrou relação entre a quantidade de recursos de segurança interna nas escolas públicas e as ocorrências de roubo ou vandalismo, e as agressões verbais e ameaças entre alunos, as ocorrências mais frequentes, não são evitadas por essas medidas.[29] Nesses conflitos, a dissuasão pela câmera pressupõe que crianças e adolescentes calculem racionalmente o risco de serem identificados antes de agir, o que dificilmente ocorre. O ataque planejado, que motivou a onda de instalação de câmeras em 2023, apresenta outro problema. Trata-se de um evento raro: foram 43 ataques entre 2001 e 2024, como visto na introdução. Sistemas desenhados para detectar eventos raros produzem um grande número de falsos alarmes, mesmo quando são precisos.[30] Quando o crime é raro, nem sequer é possível demonstrar algum benefício da vigilância. O agressor que planeja o ataque também conhece a existência das câmeras, e a câmera que registra a entrada de um atirador não impede o ataque. Nesse sentido, nem a violência cotidiana entre estudantes nem o ataque planejado preenchem as condições de que dependem os efeitos preventivos da câmera.

2.2 Espaços protegidos, dados sensíveis e pressão permanente de vigilância

A câmera impõe às pessoas observadas três ônus próprios: a pressão de saber-se observado de forma permanente, a perda de espaços de recolhimento e a exposição de dados sensíveis revelados pela simples presença em certos lugares.

No direito alemão, a vigilância permanente é, em regra, considerada desproporcional, porque submete as pessoas a uma pressão contínua de vigilância e de adaptação.[31] Essa pressão independe do funcionamento efetivo do equipamento: câmeras falsas ou desligadas produzem o mesmo efeito que câmeras em funcionamento e, por isso, também exigem aviso.[32] Ela nasce da incerteza. Quem está diante de uma câmera não sabe se está sendo observado, por quem e com que propósito.[33] O alcance e o uso das imagens são praticamente impossíveis de conhecer,

[26] PIZA, Eric L.; WELSH, Brandon C.; FARRINGTON, David P.; THOMAS, Amanda L. CCTV surveillance for crime prevention: a 40-year systematic review with meta-analysis. Criminology & Public Policy, v. 18, n. 1, p. 134-159, 2019; RATCLIFFE, Jerry H.; ROSENTHAL, Jessica M. Video surveillance of public places... 2021, p. 17 e 21.
[27] GILL, Martin; SPRIGGS, Angela. Assessing the impact of CCTV. London: Home Office Research, Development and Statistics Directorate, 2005. (Home Office Research Study, 292), p. 30; RATCLIFFE, Jerry H.; ROSENTHAL, Jessica M. Video surveillance of public places... 2021, p. 15.
[28] GILL, Martin; SPRIGGS, Angela. Assessing the impact of CCTV... 2005, p. i; RATCLIFFE, Jerry H.; ROSENTHAL, Jessica M. Video surveillance of public places... 2021, p. 19.
[29] SPOSITO, Marilia Pontes. Um breve balanço da pesquisa sobre violência escolar no Brasil. Educação e Pesquisa, São Paulo, v. 27, n. 1, 2001, p. 94 e 99.
[30] BERNAL, Paul. Data gathering, surveillance and human rights... 2016, p. 251-252; RATCLIFFE, Jerry H.; ROSENTHAL, Jessica M. Video surveillance of public places... 2021, p. 16.
[31] SEIFERT, Bernd. Videoüberwachung im künftigen Beschäftigtendatenschutzrecht: was bleibt, was geht, was kommt? Datenschutz und Datensicherheit, v. 35, n. 2, 2011, p. 105.
[32] SEIFERT, Bernd. Videoüberwachung im künftigen Beschäftigtendatenschutzrecht... 2011, p. 103.
[33] ABATE, Constantin. Präventive und repressive Videoüberwachung öffentlicher Plätze. Datenschutz und Datensicherheit, v. 35, n. 7, 2011, p. 452.

Licença *Creative Commons 3.0*

e nem sequer é fácil saber a quem a câmera pertence e a quem se dirigir.[34] Alunos ouvidos em escolas inglesas descreveram exatamente essa experiência: por não saberem se havia alguém do outro lado da tela, sentiam-se espionados.[35] A incerteza tampouco desaparece com câmeras de baixa resolução ou dirigidas a planos gerais, porque a identificação não depende do rosto. Ela pode resultar da postura, da roupa, de objetos que a pessoa carrega ou do cruzamento das imagens com outras informações, como escalas de horário.[36] Na escola, onde alunos e profissionais são conhecidos de todos e seguem horários fixos, qualquer imagem permite saber quem é quem, e a pressão se estende por todo o período em que eles permanecem ali.

Há espaços que devem ficar inteiramente livres de câmeras. No mesmo direito, a videovigilância de banheiros e vestiários é proibida em qualquer hipótese, por atingir a esfera íntima, e discute-se a extensão dessa proteção a salas de descanso e de pausa. O critério decisivo é saber se o espaço é oferecido como refúgio livre de controle.[37] A razão está nas funções que a privacidade cumpre. Ela permite que a pessoa deixe de lado, por algum tempo, os papéis que desempenha em público e recomponha-se emocionalmente.[38] Os alunos das escolas inglesas tratavam os banheiros como esse espaço de recolhimento: era para lá que iam quando queriam chorar sem ser vistos ou fazer o que não queriam expor aos colegas. Mesmo com câmeras posicionadas para não alcançar o interior das cabines, todos os alunos ouvidos consideraram sua presença uma invasão da privacidade, e alguns passaram a permanecer nesses espaços o mínimo possível.[39] A proteção desses espaços pesa ainda mais quando as pessoas observadas não podem evitar a câmera, já que a possibilidade de evitá-la e o direito de se movimentar sem ser observado integram a ponderação sobre a vigilância.[40] Durante o período escolar, os espaços de refúgio são os únicos em que alunos e profissionais exercem esse direito. Na escola, eles compreendem os banheiros e vestiários, a sala dos professores e os demais espaços em que alunos e profissionais se recolhem do convívio coletivo.

A câmera também não distingue informações irrelevantes de dados que pertencem ao núcleo da vida privada, e as escolas estão entre os lugares em que ela mais se espalhou.[41] Basta que a câmera alcance a entrada de certos espaços para que a simples frequência revele dados sensíveis. Uma câmera dirigida à porta de uma igreja, de uma sede sindical ou de um consultório especializado registra convicção religiosa, filiação sindical ou condição de saúde, sem precisar captar nada do que ocorre lá dentro. A captação desses dados deve obedecer às regras mais rigorosas aplicáveis aos dados sensíveis, e o responsável deve verificar, antes da instalação, se tais dados podem entrar no campo da câmera; muitas vezes basta mudar o ângulo ou cobrir parte da lente.[42] Na escola, a câmera que registra quem frequenta a sala de atendimento educacional especializado, a sala de orientação ou o atendimento de saúde revela informação sobre deficiência, sofrimento psíquico ou situação familiar de crianças e adolescentes.

[34] BERGFINK, Alexander. Videoüberwachung in Fahrzeugen des öffentlichen Personennahverkehrs: Besonderheiten im öffentlichen Personennahverkehr und Prüfung nach deutschem Recht. Datenschutz und Datensicherheit, v. 39, n. 3, 2015, p. 145-146.
[35] TAYLOR, Emmeline. I spy with my little eye... 2010, p. 395.
[36] BERGFINK, Alexander. Videoüberwachung in Fahrzeugen... 2015, p. 147.
[37] SEIFERT, Bernd. Videoüberwachung im künftigen Beschäftigtendatenschutzrecht... 2011, p. 104-105.
[38] TAYLOR, Emmeline. I spy with my little eye... 2010, p. 386.
[39] TAYLOR, Emmeline. I spy with my little eye... 2010, p. 393-394.
[40] BERGFINK, Alexander. Videoüberwachung in Fahrzeugen... 2015, p. 150.
[41] NGUYEN, Alexander. Videoüberwachung in sensitiven Bereichen: die Zulässigkeit der Beobachtung sensitiver Daten nach deutschem und europäischem Recht. Datenschutz und Datensicherheit, v. 35, n. 10, 2011, p. 715.
[42] NGUYEN, Alexander. Videoüberwachung in sensitiven Bereichen... 2011, p. 717.

Licença *Creative Commons 3.0*

3 RECONHECIMENTO FACIAL E DIREITOS FUNDAMENTAIS

3.1 Como funciona e onde já está em uso

O reconhecimento facial é uma tecnologia de inteligência artificial que identifica pessoas em fotos ou vídeos ao comparar seus rostos com um banco de imagens previamente formado. O sistema mede elementos do rosto, como a distância entre os olhos e a largura do nariz e da boca, transforma essas medidas em sequências numéricas e as compara com as sequências armazenadas.[43] A tecnologia acrescenta à câmera comum uma capacidade de identificação automática e em larga escala, e os dados que ela trata são biométricos, categoria que a Lei Geral de Proteção de Dados Pessoais classifica como dado pessoal sensível.[44] A identificação individual agrava o efeito inibidor descrito no item 2.2, porque permite saber quem se expressa, se reúne ou se manifesta.[45]

No Brasil, a tecnologia foi adotada na segurança pública com pouco debate e pouca informação à população. A Rede de Observatórios da Segurança registrou que, entre março e outubro de 2019, nos cinco estados monitorados, 151 pessoas haviam sido presas com uso de reconhecimento facial e que, nos casos com informação de raça e cor, 90,5% eram negras.[46] Em São Paulo, a prefeitura inaugurou em julho de 2024 a central do Smart Sampa, sistema de câmeras com reconhecimento facial que contava então com cerca de 13 mil câmeras. A contratação havia sido suspensa por decisão de primeira instância que apontou possível conflito com a Lei Geral de Proteção de Dados e risco de reforço do racismo estrutural, decisão depois derrubada em segunda instância.[47] Em 2026, a prefeitura anunciava 50 mil câmeras conectadas ao sistema, das quais 30 mil integradas por parcerias com a iniciativa privada, informando que o sistema permite o reconhecimento facial de foragidos da Justiça e que 2.956 foragidos haviam sido presos desde sua implantação.[48] O número de prisões, porém, não informa se o sistema reduz crimes. Segundo nota técnica baseada no relatório de transparência divulgado pela prefeitura em junho de 2025 e em pedidos de acesso à informação, das 1.153 prisões realizadas com o sistema até a divulgação daquele relatório, 153 foram por roubo e 540 foram classificadas pela própria prefeitura como "outros", categoria composta em mais de 90% por prisões por pensão alimentícia.[49] Uma medida que produz sensação de segurança sem demonstrar redução dos riscos aproxima-se do que Bruce Schneier chamou de teatro de segurança.[50]

A tecnologia já chegou às escolas. No Paraná, um aplicativo de reconhecimento facial é usado desde 2023 para registrar a frequência de alunos em mais de 1.700 escolas estaduais. Estudo da Unesp encontrou precisão média de 91,1%, abaixo dos 95% exigidos em contrato; as

[43] OLIVEIRA, Samuel R. de. Sorria, você está sendo filmado!: repensando direitos na era do reconhecimento facial. São Paulo: Thomson Reuters Brasil, 2020. E-book, p. RB-2.1.
[44] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais, art. 5º, II, e art. 11.
[45] OLIVEIRA, Samuel R. de. Sorria, você está sendo filmado!... 2020, p. RB-3.6.
[46] REDE DE OBSERVATÓRIOS DA SEGURANÇA. Retratos da violência: cinco meses de monitoramento, análises e descobertas. Rio de Janeiro: Centro de Estudos de Segurança e Cidadania, 2019.
[47] MELLO, Daniel. SP abre central de vigilância de câmeras com reconhecimento facial. Agência Brasil, São Paulo, 4 jul. 2024. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2024-07/sp-abre-central-de-vigilancia-de-cameras-com-reconhecimento-facial. Acesso em: 18 out. 2026.
[48] SÃO PAULO (Município). Smart Sampa chega a 50 mil câmeras e já supera em 25% o previsto no Programa de Metas. São Paulo: Prefeitura de São Paulo, 1 abr. 2026. Disponível em: https://prefeitura.sp.gov.br/web/seguranca_urbana/w/smart-sampa-chega-a-50-mil-c%C3%A2meras-e-j%C3%A1-supera-em-25-o-previsto-no-programa-de-metas. Acesso em: 18 out. 2026.
[49] BOEHM, Camila. Pesquisa aponta problemas e prisões indevidas a partir do Smart Sampa. Agência Brasil, São Paulo, 4 fev. 2026. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2026-02/pesquisa-aponta-problemas-e-prisoes-indevidas-partir-do-smart-sampa. Acesso em: 18 out. 2026.
[50] SCHNEIER, Bruce. Beyond fear: thinking sensibly about security in an uncertain world. New York: Copernicus Books, 2003.

Licença *Creative Commons 3.0*

imagens são armazenadas em servidores do governo por um ano; e o Ministério Público estadual ajuizou ação por violação da Lei Geral de Proteção de Dados.[51] A frequência escolar, além disso, é condição para benefícios sociais, o que dá ao registro biométrico de presença consequências que vão além da gestão escolar. Em Campinas, projeto de lei noticiado em outubro de 2026 propõe um programa de controle de acesso às escolas municipais por reconhecimento facial de alunos, professores e funcionários, com uso dos registros também para acompanhar a frequência e prevenir a evasão.[52]

3.2 Interseções entre o reconhecimento facial e a teoria do Black Opticon

O reconhecimento facial erra, e o erro, na segurança pública, se traduz em abordagens e prisões de pessoas inocentes.[53] O erro tampouco se distribui de modo uniforme: estudo sobre sistemas comerciais de classificação de gênero a partir do rosto encontrou taxas de erro de até 34,7% para mulheres de pele mais escura, contra menos de 1% para homens de pele mais clara.[54] Os números sobre prisões realizadas com o uso de reconhecimento facial, apresentados no item 4.1, admitem uma explicação que vai além do erro técnico. Anita Allen propôs a noção de "Black Opticon" para descrever os custos que o uso de plataformas e tecnologias orientadas por dados impõe, de forma desproporcional, à população negra, bem como a outros grupos historicamente escravizados e subordinados.[55] Ao tratar as falhas de privacidade e de proteção de dados como violações de direitos civis, a autora identifica três formas de discriminação: a hipervigilância discriminatória, que faz da população negra o alvo preferencial da vigilância excessiva; a exclusão discriminatória, que afasta essa população de oportunidades com base na raça; e a predação discriminatória, que consiste no uso de dados pessoais para direcionar golpes e fraudes a pessoas em situação de vulnerabilidade.[56]

Ao aplicar essas categorias à realidade brasileira, Monagreda aponta o uso de câmeras de reconhecimento facial na Bahia, estado com a maior população negra do país, como a prática que melhor ilustra a hipervigilância discriminatória, e observa que a população negra está sub-representada nos conjuntos de dados que treinam os sistemas e sobrerrepresentada nas bases de suspeição, oriundas dos próprios sistemas com que são confrontados.[57] A autora acrescenta que a vigilância concentrada em determinados territórios produz os próprios dados que depois orientam novas ações de vigilância sobre eles mesmos, de modo que a tecnologia tende a confirmar a seletividade existente antes de sua implantação.[58]

---

[51] SCHMIDT, Nico; COELHO, Leonardo. 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: 18 out. 2026.

[52] MORAIS, Larissa de. Escolas de Campinas terão reconhecimento facial? Entenda PL. ACidade ON Campinas, Campinas, 7 out. 2026. Disponível em: https://www.acidadeon.com/campinas/politica/escolas-de-campinas-terao-reconhecimento-facial-entenda-pl/. Acesso em: 18 out. 2026.

[53] ALLEN, Anita L. Dismantling the "Black Opticon": privacy, race equity, and online data-protection reform. The Yale Law Journal Forum, v. 131, 2022, p. 939.

[54] BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, v. 81, 2018, p. 77.

[55] ALLEN, Anita L. Dismantling the "Black Opticon"... 2022, p. 907 e 911. A noção é aplicada à realidade brasileira por MONAGREDA, Johanna K. Por que falar de raça quando falamos de dados pessoais, inteligência artificial e algoritmos? In: GONÇALVES, Adriana; TORRE, Luísa; MELO, Paulo Victor (ed.). Inteligência artificial e algoritmos: desafios e oportunidades para os media. Covilhã: LabCom, 2024, p. 106.

[56] ALLEN, Anita L. Dismantling the "Black Opticon"... 2022, p. 913-914, 917 e 924; MONAGREDA, Johanna K. Por que falar de raça... 2024, p. 118.

[57] MONAGREDA, Johanna K. Por que falar de raça... 2024, p. 120-121.

[58] MONAGREDA, Johanna K. Por que falar de raça... 2024, p. 121-122. No mesmo sentido, ALLEN, Anita L. Dismantling the "Black Opticon"... 2022, p. 927; CITRON, Danielle Keats; SOLOVE, Daniel J. Privacy harms... 2021, p. 30.

Licença *Creative Commons 3.0*

O raciocínio aplica-se à escola, onde a exclusão discriminatória descrita por Allen ganha relevância particular. No Paraná, como visto no item 4.1, a precisão abaixo da exigida em contrato e a vinculação da frequência a benefícios sociais fazem com que os erros de identificação recaiam sobre as famílias que mais dependem dessas políticas. Monagreda registra que, no Bolsa Família, a coleta de dados das beneficiárias, em sua maioria mulheres negras, foi conduzida sob a presunção de que elas tentariam fraudar o sistema, com pouca explicação sobre o uso das informações, e que essas mesmas beneficiárias já foram alvo de golpes, além de vítimas de desinformação e de propaganda política dirigida.[59] Como a raça não precisa aparecer como critério explícito para orientar a discriminação, uma vez que informações como endereço, nome e renda permitem inferi-la, uma norma escolar que sequer menciona raça pode produzir os efeitos de exclusão que Allen descreve.[60]

Esse problema alcança também estudantes transgênero e não binários, pois o relatório da Oxfam sobre gênero e tecnologia registra que os sistemas biométricos tendem a identificar seus corpos e suas identidades como enganosos, expondo-os a erros de identificação e a situações de constrangimento que, no ambiente escolar, atingem diretamente direitos assegurados pelo Estatuto da Criança e do Adolescente, em especial a preservação da imagem e da identidade.[61]

Essas contribuições oferecem à proibição do reconhecimento facial nas escolas um fundamento próprio, ligado à não discriminação. Monagreda observa que, quando a justiça social é tomada como parte do problema a ser resolvido, pode-se concluir que alguns usos da tecnologia, como o reconhecimento facial na segurança pública, devem ser simplesmente banidos.[62] Levar essa tecnologia à escola pública significa, portanto, estender aos estudantes a mesma lógica de vigilância que já recai de forma seletiva sobre determinados territórios, agora em um espaço que o ordenamento jurídico reserva à formação e à proteção integral.

4 O DECRETO DE CAMPINAS: AS CÂMERAS DO PROTOCOLO ÉGIDE

4.1 Origem e alcance

O Protocolo Égide foi instituído pelo Decreto nº 22.759, de 27 de abril de 2023, como Programa Municipal de Prevenção contra a Prática de Atentados Violentos nas Dependências das Escolas Municipais, com fundamento na Lei municipal nº 16.318/2022. O desenho original do programa combinava protocolos de resposta a emergências, formação de profissionais, campanhas contra o bullying e um componente tecnológico de grande porte, com câmeras ligadas à central de monitoramento municipal e previsão de recursos analíticos capazes de apontar comportamentos considerados fora do padrão. Avaliação conduzida com professores, gestores escolares e gestores das secretarias concluiu que o programa cumpriu a instalação do

[59] MONAGREDA, Johanna K. Por que falar de raça... 2024, p. 108-109 e 119.
[60] MONAGREDA, Johanna K. Por que falar de raça... 2024, p. 119. No mesmo sentido, ALLEN, Anita L. Dismantling the "Black Opticon"... 2022, p. 921-922; CITRON, Danielle Keats; SOLOVE, Daniel J. Privacy harms... 2021, p. 36.
[61] CEIA, Vanessa; NOTHWEHR, Benji; WAGNER, Liz. Género y tecnología: un análisis interseccional de las tendencias claves con el enfoque de derechos. Boston: Oxfam America, 2021, p. 39.
[62] MONAGREDA, Johanna K. Por que falar de raça... 2024, p. 128.

Licença Creative Commons 3.0

sistema de monitoramento na maior parte das escolas, não avançou nos demais eixos e é considerado inativo pelos participantes.[63] A câmera, portanto, foi o que restou da política.

O Decreto nº 24.328, de 5 de março de 2026, publicado no Diário Oficial do Município no dia seguinte, veio quase três anos depois do início do programa. Ele estabelece princípios e parâmetros para a instalação de câmeras de monitoramento circunscritas ao Protocolo Égide nas escolas do sistema municipal de ensino e define procedimentos e atribuições para o tratamento, o uso e a destinação das imagens.[64] Aplica-se aos Centros de Educação Infantil geridos pela Secretaria Municipal de Educação ou em cogestão com organizações da sociedade civil, às escolas municipais de ensino fundamental, de tempo integral e de educação de jovens e adultos, e às unidades mantidas pela Fundação Municipal para Educação Comunitária (Fumec).[65] A instalação resulta de ação conjunta das Secretarias de Educação, de Cooperação nos Assuntos de Segurança Pública e de Gestão de Pessoas e da Fumec (art. 4º).

O caráter tardio do decreto aparece em seu próprio texto. O artigo 29 valida todos os procedimentos do Protocolo Égide implementados nas escolas antes de sua vigência, e o artigo 8º descreve as etapas de implantação como um processo em curso desde 2023, fixando prazo de 120 dias para que as escolas ainda não concluídas terminem a instalação.[66] A regulação, assim, disciplinou e convalidou uma rede já instalada, sem condicionar a instalação a qualquer exame prévio.

4.2 Princípios e limites espaciais

O artigo 5º enumera os princípios que regem o tratamento das imagens: respeito à individualidade e à privacidade de estudantes e profissionais; proteção integral de crianças e adolescentes, nos termos do Estatuto da Criança e do Adolescente; finalidade específica; proporcionalidade e razoabilidade; transparência quanto à existência, à localização e à finalidade das câmeras; sigilo e controle de acesso; armazenamento seguro e temporário; e conformidade com a legislação de proteção de dados. A finalidade específica é definida como a utilização das imagens restrita às situações relacionadas à segurança escolar e à apuração de incidentes e potenciais ameaças de que trata o programa municipal de prevenção a atentados.[67]

O artigo 6º contém a regra mais relevante do decreto. As câmeras podem ser instaladas nas áreas comuns e de grande circulação de pessoas, e é vedada a instalação em uma lista de espaços que varia conforme o tipo de escola. Nos Centros de Educação Infantil, são excluídos o berçário, a sala de aula, o fraldário, as salas da direção e da coordenação pedagógica e os sanitários. Nas escolas de ensino fundamental e de educação de jovens e adultos, a lista abrange a biblioteca, os laboratórios, a sala de audiovisual, a sala de aula, a sala de recursos multifuncionais, a sala de educação física, a sala dos professores, as salas administrativas e os sanitários. Nas unidades da Fumec, abrange a sala de leitura, os laboratórios, a sala de aula, a sala de recursos multifuncionais, a sala dos professores, as salas administrativas e os sanitários.[68]

[63] PESCI, Helio de Souza. Avaliação da implementação e execução do Protocolo Égide no âmbito das escolas municipais de Campinas (SP). 2026. Dissertação (Mestrado em Educação) – Pontifícia Universidade Católica de Campinas, Campinas, 2026.
[64] CAMPINAS. Decreto nº 24.328, de 5 de março de 2026. Diário Oficial do Município de Campinas, n. 13.780, 6 mar. 2026, ementa.
[65] CAMPINAS. Decreto nº 24.328/2026, art. 3º.
[66] CAMPINAS. Decreto nº 24.328/2026, arts. 8º, § 2º, e 29.
[67] CAMPINAS. Decreto nº 24.328/2026, art. 5º, III.
[68] CAMPINAS. Decreto nº 24.328/2026, art. 6º.

Licença *Creative Commons 3.0*

A lista corresponde, em boa medida, aos parâmetros do item 3.2. Ela preserva os espaços de ensino, a sala dos professores, que funciona como refúgio dos profissionais, os espaços de intimidade corporal, como sanitários e fraldários, e a sala de recursos multifuncionais, cuja frequência revela a condição de deficiência de estudantes. O decreto, entretanto, abre uma exceção relevante. Segundo o parágrafo único do artigo 6º, os locais indicados nos incisos, bem como outras câmeras instaladas antes da vigência do decreto, poderão ser integrados ao Protocolo Égide mediante análise e autorização da comissão de implantação, desde que sua instalação e o monitoramento atendam integralmente ao decreto.[69] A redação permite que os próprios espaços vedados pelo caput recebam câmeras integradas ao programa por decisão administrativa, sem critério material que oriente essa decisão.

4.3 Fluxo das imagens, acesso e retenção

O artigo 11 define o fluxo das imagens: elas são espelhadas, em tempo real, para o Centro Integrado de Comando e Controle (CICC), órgão da área de segurança pública, e ficam armazenadas no equipamento de gravação de cada escola.[70] O compartilhamento não é autorizado; o acesso, quando necessário, é de competência exclusiva e intransferível do diretor educacional ou, nas unidades da Fumec, do titular do departamento responsável; e a disponibilização das imagens fica restrita à Procuradoria-Geral do Município e ao atendimento de ofícios de tribunais e de autoridade policial. Em situações atípicas ou graves, o diretor deve reservar imediatamente as imagens. O artigo 12 fixa o armazenamento por no mínimo 15 e no máximo 45 dias, após o que as imagens são sobrescritas automaticamente, salvo as reservadas ou requisitadas por autoridade competente.

Os limites de acesso, porém, recaem sobre o armazenamento local. O espelhamento em tempo real para o CICC significa que a central de segurança recebe as imagens de todas as escolas conectadas, e o artigo 13 atribui à Secretaria de Cooperação nos Assuntos de Segurança Pública, por meio do CICC, a tarefa de monitorar as imagens geradas pelas escolas, conforme os recursos agregados às câmeras, que possibilitam a gravação ou a seletividade das imagens, e de acionar a Guarda Municipal conforme as ocorrências.[71] O decreto não define o que são esses recursos de seletividade nem proíbe expressamente funções de análise automatizada ou de reconhecimento facial. Também não fixa regras de retenção, de acesso ou de registro para as imagens que circulam no CICC, e atribui ao departamento de informática o estudo da viabilidade de migrar o tratamento das imagens para um servidor específico (art. 14, III), o que indicaria centralização futura do armazenamento.

4.4 Governança e participação

A implantação e o acompanhamento cabem a uma comissão formada por servidores das Secretarias de Educação, de Segurança Pública e de Gestão de Pessoas e da Fumec, coordenada pela assessoria de tecnologia educacional, com reuniões a cada dois meses.[72] Compete a ela acompanhar a instalação, definir critérios de avaliação, analisar a incorporação de câmeras anteriores ao decreto, decidir casos omissos e elaborar relatórios. A comissão é interna à administração e não inclui representantes da comunidade escolar, do Conselho Municipal dos Direitos da Criança e do Adolescente ou de órgão independente de proteção de dados. A

[69] CAMPINAS. Decreto nº 24.328/2026, art. 6º, parágrafo único.
[70] CAMPINAS. Decreto nº 24.328/2026, art. 11.
[71] CAMPINAS. Decreto nº 24.328/2026, art. 13, III e IV.
[72] CAMPINAS. Decreto nº 24.328/2026, arts. 25 e 26.

Licença *Creative Commons 3.0*

participação da comunidade se limita a ser informada sobre as finalidades das câmeras (art. 8º, § 1º) e à aprovação, pelo Conselho de Escola, do plano de aplicação dos recursos para a compra dos equipamentos (art. 22, II), o que submete ao conselho apenas a forma de gastar os recursos; a decisão de vigiar não passa por ele. O decreto ainda determina que o departamento de apoio às escolas encaminhe providências administrativas contra as escolas que não viabilizarem a implantação do Protocolo Égide, independentemente dos motivos causadores.[73]

5 OS MODELOS DE SÃO PAULO E DE SÃO JOSÉ DO RIO PRETO

5.1 São Paulo: a escola dentro do Smart Sampa

O município de São Paulo não editou norma específica sobre câmeras em escolas. As câmeras das unidades municipais de ensino foram incorporadas ao Programa Smart Sampa, instituído pelo Decreto nº 63.552, de 4 de julho de 2024, sob coordenação da Secretaria Municipal de Segurança Urbana. O decreto cria uma rede de câmeras de vigilância inteligente em locais estratégicos, integrada aos serviços de segurança e de emergência, e prevê a integração de câmeras públicas e privadas.[74] Como visto no item 4.1, o sistema opera reconhecimento facial e em 2026 reunia 50 mil câmeras.

A governança do programa está a cargo de um Conselho de Gestão e Transparência, presidido pela Secretaria de Segurança Urbana e composto também pela Controladoria Geral do Município e pela Secretaria de Justiça, ao qual cabe aprovar bancos de dados, entidades que podem receber dados e níveis de acesso às imagens, além de publicar relatórios.[75] O decreto proíbe a venda e o compartilhamento dos dados coletados, salvo nas hipóteses autorizadas pelo conselho, determina a anonimização dos dados não vinculados a investigações, exige capacitação dos operadores em direitos humanos e racismo, cria uma ouvidoria e prevê revisão abrangente do programa em cinco anos.[76] A previsão de relatório de impacto à proteção de dados aparece de forma condicionada a eventuais necessidades (art. 11, parágrafo único).

A inserção das escolas nesse sistema foi feita pela Portaria Conjunta SME/SMSU nº 4, de 12 de dezembro de 2024. A portaria disciplina o fluxo de instalação e manutenção das câmeras nas unidades educacionais, a cargo da Secretaria de Segurança Urbana, com aprovação do cronograma pela área de proteção escolar da Secretaria de Educação.[77] Seus anexos indicam 179 unidades a serem incluídas no programa com recursos da educação e 366 unidades já atendidas com recursos da segurança urbana. Às escolas cabe indicar um responsável, informar falhas, acompanhar os serviços e definir, com a Secretaria de Segurança Urbana, as áreas prioritárias de monitoramento, considerando o histórico de ocorrências e as vulnerabilidades estruturais da unidade, além dos horários de monitoramento.[78]

O capítulo da portaria dedicado à proteção de dados repete compromissos gerais: respeito aos direitos de liberdade, de privacidade e de personalidade previstos na Lei Geral de Proteção de Dados, uso das imagens restrito à segurança das unidades, do patrimônio, dos servidores e dos estudantes, eliminação de dados a pedido e responsabilidade das secretarias por

[73] CAMPINAS. Decreto nº 24.328/2026, art. 21, II.
[74] SÃO PAULO (Município). Decreto nº 63.552, de 4 de julho de 2024. Institui o Programa Smart Sampa, arts. 1º, 2º e 4º.
[75] SÃO PAULO (Município). Decreto nº 63.552/2024, arts. 6º e 7º.
[76] SÃO PAULO (Município). Decreto nº 63.552/2024, arts. 7º, X, 8º, 12, 16 e 21.
[77] SÃO PAULO (Município). Secretaria Municipal de Educação; Secretaria Municipal de Segurança Urbana. Portaria Conjunta SME/SMSU nº 4, de 12 de dezembro de 2024, arts. 1º a 4º.
[78] SÃO PAULO (Município). Portaria Conjunta SME/SMSU nº 4/2024, art. 6º.

Licença *Creative Commons 3.0*

danos.[79] A divulgação de imagens depende de autorização do Conselho de Gestão e Transparência do Smart Sampa (art. 16). A portaria não indica espaços em que a instalação é vedada, não fixa prazo de retenção, não trata do espelhamento para a central do programa, não menciona o Estatuto da Criança e do Adolescente e não exclui as câmeras escolares das funções de reconhecimento facial e de análise que o programa oferece. As regras aplicáveis às imagens de crianças são, portanto, as regras gerais de uma plataforma de segurança urbana, decididas por um conselho presidido pela própria secretaria de segurança.

5.2 São José do Rio Preto: a câmera na sala de aula

O terceiro modelo nasceu no Poder Legislativo. A Lei nº 12.953/2018, de São José do Rio Preto, dispõe sobre a instalação de câmeras de monitoramento de segurança nas creches e escolas públicas municipais, incluindo as salas de aula.[80] O prefeito propôs ação direta de inconstitucionalidade contra a lei, e o Órgão Especial do Tribunal de Justiça de São Paulo, por maioria de votos, julgou a ação improcedente.[81]

O fundamento do relator, desembargador Salles Rossi, merece atenção porque resume a concepção de escola que sustenta a vigilância. Segundo o voto, escolas são "locais públicos onde os serviços prestados também são de natureza e de interesse público", de modo que o monitoramento "não atinge a intimidade ou privacidade daqueles que ali se encontram"; além disso, o monitoramento se limitaria ao armazenamento das imagens, "cuja exibição será solicitada apenas em caso específico".[82] A decisão também foi lida como reconhecimento de que a autonomia administrativa da escola permite instalar câmeras inclusive em salas de aula.[83]

Parecer da assessoria jurídica da Câmara Municipal de São Paulo, ao examinar proposta de câmeras em um centro de educação infantil, distinguiu o caso de São José do Rio Preto da transmissão de imagens em tempo real a famílias. Segundo o parecer, o precedente do Tribunal tratou de monitoramento para fins de segurança, em que as imagens ficam armazenadas e não são exibidas automaticamente, e a transmissão contínua de imagens de crianças exigiria consentimento expresso de professores e responsáveis, aviso em todas as áreas monitoradas e controles de acesso.[84] O parecer também registrou que a vigilância constante inibe a espontaneidade e produz uma espécie de liberdade monitorada em sala de aula, embora não tenha considerado essa restrição suficiente para violar a liberdade de ensinar.

O modelo de São José do Rio Preto é, assim, o mais invasivo no espaço, porque alcança a sala de aula, e o mais restrito no uso declarado das imagens, porque o fundamento da decisão judicial foi a ausência de exibição fora de casos específicos.

[79] SÃO PAULO (Município). Portaria Conjunta SME/SMSU nº 4/2024, arts. 7º a 11.
[80] CÂMARA MUNICIPAL DE SÃO PAULO. Assessoria Jurídica. Parecer ADM nº 035/2019. São Paulo, 2019.
[81] SÃO PAULO (Estado). Tribunal de Justiça. Órgão Especial. Ação Direta de Inconstitucionalidade nº 2113734-65.2018.8.26.0000. Relator: Des. Salles Rossi. São Paulo, 2018.
[82] TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. Mantida lei sobre instalação de câmeras em escolas de Rio Preto. São Paulo, 28 set. 2018. Disponível em: https://www.tjsp.jus.br/Noticias/Noticia?codigoNoticia=53595&pagina=1. Acesso em: 18 out. 2026.
[83] SANTOS, Ana Luiza; JACOBS, Edgar. Instalação de câmeras de segurança em instituições de ensino é considerada constitucional pelo TJSP. Jacobs Consultoria, 26 abr. 2022. Disponível em: https://www.jacobsconsultoria.com.br/post/instala%C3%A7%C3%A3o-de-c%C3%A2meras-de-seguran%C3%A7a-em-institui%C3%A7%C3%B5es-de-ensino-%C3%A9-considerada-constitucional-pelo-tjsp. Acesso em: 18 out. 2026.
[84] CÂMARA MUNICIPAL DE SÃO PAULO. Parecer ADM nº 035/2019.

Licença Creative Commons 3.0

6 COMPARAÇÃO DOS MODELOS

6.1 Parâmetros de comparação

A comparação toma como critérios os parâmetros extraídos nas seções 2 a 4 para avaliar uma medida de vigilância. São eles: a exigência de justificativa concreta antes da instalação; a delimitação dos espaços de ensino, de intimidade, de refúgio e de frequência reveladora de dados sensíveis; o controle da coleta e do processamento das imagens, inclusive de seu fluxo para centrais de segurança e de funções de identificação automática; a retenção; a governança, isto é, quem decide e fiscaliza e com que independência; e a consideração da condição peculiar dos titulares, crianças e adolescentes, cujo tratamento de dados deve observar o seu melhor interesse.[85]

Este último parâmetro tem fundamento constitucional e legal próprio. O Estatuto da Criança e do Adolescente define o direito ao respeito como a inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, abrangendo a preservação da imagem, da identidade, da autonomia e dos espaços e objetos pessoais, e impõe a todos o dever de pô-los a salvo de qualquer tratamento vexatório ou constrangedor.[86] A Autoridade Nacional de Proteção de Dados, por sua vez, firmou entendimento de que o tratamento de dados de crianças e adolescentes pode se apoiar nas bases legais gerais da lei, desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto.[87] A Constituição assegura, ainda, a liberdade de aprender e de ensinar como princípio do ensino.[88] A escola é, portanto, um espaço juridicamente qualificado, e sua vigilância não pode ser avaliada pelos mesmos critérios aplicados a uma praça ou a uma estação de metrô.

6.2 Três graus de incorporação da escola à segurança urbana

A comparação mostra que os três modelos convergem em um ponto e divergem em outro. Convergem porque nenhum deles exige justificativa prévia e concreta para a instalação. Em Campinas, a câmera é obrigatória; em São Paulo, a escola define apenas as áreas prioritárias de monitoramento; em São José do Rio Preto, a lei impõe as câmeras a todas as unidades.

Os modelos divergem no grau em que incorporam a escola ao aparato de segurança urbana. Campinas ocupa posição intermediária e ambígua. O decreto tem a delimitação espacial mais cuidadosa dos três modelos, menciona a proteção integral e fixa retenção e regras de acesso; ao mesmo tempo, espelha as imagens em tempo real para uma central de segurança sem regras para seu tratamento ali, admite recursos de seletividade não definidos e permite que a comissão autorize câmeras nos espaços vedados.

São Paulo representa o grau máximo de incorporação. Como visto no item 6.1, as imagens escolares seguem as regras gerais de uma plataforma criada para vigiar a cidade, com reconhecimento facial e câmeras privadas integradas. A criança que entra na escola, do ponto de vista dos dados, entra no mesmo sistema que vigia uma estação ou uma rua comercial. Esse é o cenário em que os riscos de classificação e seleção de pessoas, examinados no item 2.1, encontram condições técnicas para se concretizarem no espaço escolar. A esses riscos soma-se a hipervigilância discriminatória examinada no item 4.2.

[85] BRASIL. Lei nº 13.709/2018, art. 14.
[86] BRASIL. Lei nº 8.069, de 13 de julho de 1990. Estatuto da Criança e do Adolescente, arts. 17 e 18.
[87] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Enunciado CD/ANPD nº 1, de 22 de maio de 2023.
[88] BRASIL. Constituição da República Federativa do Brasil de 1988, art. 206, II.

Licença *Creative Commons 3.0*

São José do Rio Preto representa um modelo diferente, de vigilância local e intensa. A lei leva a câmera ao interior da sala de aula, o espaço em que se exercem a liberdade de aprender e de ensinar e em que professores e alunos passam a maior parte do dia, e cria a pressão permanente de vigilância examinada no item 3.2.

6.3 O que as normas regulam e o que deixam de regular

Os três modelos compartilham um defeito de construção que a comparação dos detalhes tende a esconder. Todos regulam a vigilância a partir de seu ponto final, o acesso humano às gravações, e deixam sem disciplina as decisões que o antecedem: se a escola deve ser vigiada, com que finalidade, sob qual regime jurídico e sob o controle de quem. Esse defeito se desdobra em sete falhas. As quatro primeiras são dogmáticas e dizem respeito ao regime jurídico do tratamento das imagens, à forma do ato que o institui, ao exame de proporcionalidade e à premissa de que a coleta não atinge direitos. A quinta é teórica e diz respeito à relação de poder criada pela instalação. As duas últimas dizem respeito aos limites do sistema: a finalidade aberta, que não impede sua expansão funcional, e o melhor interesse de crianças e adolescentes, que as normas não avaliam.

A primeira falha é a indefinição do regime jurídico aplicável. A Lei Geral de Proteção de Dados oferece dois caminhos ao poder público. Se o tratamento de imagens integra a prestação do serviço educacional, ele se submete à lei: deve atender à finalidade pública e às competências legais do órgão, respeitar os princípios da finalidade e da necessidade, observar o melhor interesse da criança e pode ser objeto de relatório de impacto exigido pela autoridade nacional.[89] Se o tratamento se destina à segurança pública, a lei o exclui de seu âmbito e exige lei específica, que preveja medidas proporcionais e estritamente necessárias ao interesse público, além de atribuir à autoridade nacional o dever de solicitar relatórios de impacto aos responsáveis.[90] Essa lei não existe. As normas municipais oscilam entre os dois regimes sem escolher nenhum. Campinas declara conformidade com a Lei Geral de Proteção de Dados, mas define a finalidade das imagens pela apuração de incidentes e potenciais ameaças, envia as imagens em tempo real a um órgão de segurança e atribui a esse órgão o dever de acionar a Guarda Municipal.[91] São Paulo insere as escolas em um programa da Secretaria de Segurança Urbana. São José do Rio Preto impôs as câmeras em nome da segurança. O resultado é um tratamento de dados com finalidade de segurança pública executado sob um regime nominalmente educacional, que escapa ao mesmo tempo das exigências do artigo 4º, § 1º, e da aplicação integral da lei.

A segunda falha diz respeito à forma do ato. Desde a Emenda Constitucional nº 115/2022, a proteção de dados pessoais é direito fundamental expresso, e a competência para legislar sobre a proteção e o tratamento de dados pessoais é privativa da União.[92] Os municípios podem organizar seus serviços e executar a lei federal; não podem criar, por decreto ou por portaria, a base legal que a própria lei federal reservou a uma lei específica. A coleta contínua de imagens de toda a população escolar é, além disso, uma restrição permanente aos direitos à intimidade, à imagem e à proteção de dados, e restrições dessa natureza dependem de lei que defina com precisão sua finalidade, seus limites e suas garantias. Ao suspender a medida provisória que determinava o compartilhamento de dados de usuários de telefonia com o IBGE, o Supremo Tribunal Federal considerou insuficiente uma norma que não delimitava com

[89] BRASIL. Lei nº 13.709/2018, arts. 6º, I e III, 14, 23 e 38.
[90] BRASIL. Lei nº 13.709/2018, art. 4º, III, a, e §§ 1º e 3º.
[91] CAMPINAS. Decreto nº 24.328/2026, arts. 5º, III e VIII, 11 e 13, III e IV.
[92] BRASIL. Constituição da República Federativa do Brasil de 1988, art. 5º, LXXIX, e art. 22, XXX, incluídos pela Emenda Constitucional nº 115, de 10 de fevereiro de 2022.

Licença Creative Commons 3.0

precisão a finalidade e o modo de uso dos dados nem previa garantias contra seu uso indevido.[93] Campinas e São Paulo instituíram a vigilância escolar por atos infralegais, e São José do Rio Preto o fez por lei que, segundo as fontes disponíveis, determina a instalação sem definir finalidade específica, retenção ou controle. Nos três casos, a forma do ato é incompatível com a intensidade da restrição.

A terceira falha é a inversão da proporcionalidade. O exame de proporcionalidade é relativo a uma situação concreta: a adequação e a necessidade de uma câmera só podem ser avaliadas diante do risco específico do local onde ela será instalada.[94] Uma norma que impõe câmeras a todas as escolas torna esse exame impossível, porque decide a necessidade em abstrato e de uma vez para todas as situações. Campinas vai além. O decreto enuncia a proporcionalidade entre seus princípios e, no mesmo texto, determina providências administrativas contra as escolas que não viabilizarem a implantação, independentemente dos motivos.[95] As razões que uma escola poderia apresentar para não instalar câmeras, como a ausência de risco ou a existência de meio menos invasivo, são exatamente as razões que o exame de necessidade exige considerar, e o decreto as declara irrelevantes. O ônus da justificação inverte-se: a administração não precisa demonstrar por que vigia, e a escola precisa responder por não vigiar. Em São José do Rio Preto, a lei estendeu a obrigação à sala de aula, e o controle judicial limitou-se à premissa de que a privacidade não se aplica a lugar público, sem examinar se havia meio menos gravoso para atingir o fim declarado. Em São Paulo, a única escolha deixada à escola é a das áreas prioritárias, o que diz respeito a onde vigiar, deixando intocada a decisão de vigiar.

A quarta falha está na premissa, comum aos três modelos e explicitada pelo Tribunal de Justiça, de que a coleta e o armazenamento não atingem direitos enquanto as imagens não forem exibidas. Essa premissa é incompatível com o direito positivo brasileiro. A Constituição protege a imagem das pessoas, sem distinguir o local em que é captada; o Estatuto da Criança e do Adolescente protege a imagem, como visto no item 7.1; e a proteção de dados pessoais recai sobre o dado e sobre a pessoa a quem ele se refere, qualquer que seja o espaço em que foi coletado.[96] As regras de acesso dos três modelos protegem contra a divulgação indevida das imagens. A intervenção nos direitos já ocorreu quando as imagens foram captadas, armazenadas e, em Campinas e em São Paulo, enviadas a uma central de segurança; para essa intervenção, os modelos não oferecem justificativa nem limite.

A quinta falha é teórica e explica por que as regras de acesso, mesmo quando rigorosas, não resolvem o problema. Regras de acesso limitam as ocasiões em que alguém olha as imagens; elas deixam intacta a capacidade de olhar. Como visto no item 2.2, a liberdade depende de arranjos institucionais que retirem essa capacidade de quem pode exercê-la sem controle. Os três modelos deixam a capacidade com o aparato de segurança e a submetem a controles internos à própria administração: em Campinas, uma comissão de servidores; em São Paulo, um conselho presidido pela secretaria que opera as câmeras; em São José do Rio Preto, nenhum controle identificável nas fontes consultadas. A pergunta sobre quem controla os controladores recebe nos três casos a resposta de que os controladores controlam a si mesmos.[97]

[93] BRASIL. Supremo Tribunal Federal. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387. Relatora: Min. Rosa Weber. Tribunal Pleno, julgado em 7 maio 2020.
[94] AGUSTINA, José R.; GALDON CLAVELL, Gemma. The impact of CCTV on fundamental rights... 2011, p. 169.
[95] CAMPINAS. Decreto nº 24.328/2026, arts. 5º, IV, e 21, II.
[96] BRASIL. Constituição da República Federativa do Brasil de 1988, art. 5º, X e LXXIX.
[97] AGUSTINA, José R.; GALDON CLAVELL, Gemma. The impact of CCTV on fundamental rights... 2011, p. 170.

Licença *Creative Commons 3.0*

A sexta falha é a ausência de limite à expansão funcional do sistema. A finalidade declarada em Campinas, a apuração de incidentes e de potenciais ameaças, não tem limite interno, porque, na lógica da gestão de riscos, comportamentos comuns podem ser lidos como sinal de ameaça.[98] Uma finalidade assim formulada não atende à exigência legal de propósitos específicos e explícitos e funciona como uma autorização aberta. A falta de uma regra para a identificação automática agrava o problema. O decreto de Campinas admite recursos de seletividade das imagens sem defini-los, São Paulo já opera reconhecimento facial na plataforma a que as escolas foram integradas, e a Câmara Municipal de Campinas examina projeto que propõe reconhecimento facial nas escolas municipais. A infraestrutura instalada permite que a mudança ocorra por meio de contratação de software ou por ato administrativo, sem nova lei[99], e o caso do Paraná, examinado no item 4.2, mostra aonde essa expansão pode levar.

A última falha é a redução do melhor interesse da criança a uma declaração. Como visto no item 7.1, a Autoridade Nacional de Proteção de Dados exige que o melhor interesse de crianças e adolescentes seja avaliado no caso concreto. Nenhum dos modelos prevê essa avaliação. Campinas menciona a proteção integral entre seus princípios e não a converte em requisito de nenhuma decisão; São Paulo e São José do Rio Preto nem sequer a mencionam. O melhor interesse passa a ser presumido, o que equivale a dispensá-lo. A frequência escolar obrigatória torna o consentimento ilusório, e o dever, referido no item 7.1, de pôr crianças e adolescentes a salvo de tratamento vexatório ou constrangedor alcança a vigilância permanente de seus corpos e gestos no espaço em que são obrigados a permanecer.

CONCLUSÃO

O artigo comparou três modelos de regulação municipal de câmeras em escolas no estado de São Paulo e sustentou que todos eles regularam o funcionamento das câmeras e deixaram sem resposta a questão que deveria anteceder a instalação. Nenhum dos modelos exige a demonstração de um risco concreto, da capacidade da câmera de reduzi-lo e da inexistência de meio menos invasivo.

Os resultados permitem indicar o que uma regulação adequada deveria conter. A instalação de câmeras em cada escola deveria depender de justificativa concreta, de relatório de impacto à proteção de dados e de manifestação da comunidade escolar, com avaliação periódica de eficácia e prazo de vigência. Os espaços de ensino, de intimidade, de refúgio dos profissionais e de atendimento especializado deveriam ser excluídos sem exceção administrativa. O reconhecimento facial e outras formas de identificação automática deveriam ser proibidos nas escolas. O fluxo de imagens para centrais de segurança deveria ser excepcional e submetido às mesmas regras de retenção e acesso aplicadas na escola. E o controle deveria caber a instância com participação da comunidade escolar e de órgãos de defesa dos direitos da criança, independente da área de segurança.

Para o Protocolo Égide, essas conclusões têm consequência específica. O componente de vigilância foi o único efetivamente implantado, enquanto os eixos de formação e de prevenção ligados ao cotidiano escolar ficaram para trás. Como mostrado no item 3.1, a câmera

[98] LYON, David. Surveillance, security and social sorting... 2007, p. 162-163. No mesmo sentido, HOROWITZ, Sarah. Foucault's Panopticon... 2017, p. 46; BERNAL, Paul. Data gathering, surveillance and human rights... 2016, p. 257-258.
[99] BERNAL, Paul. Data gathering, surveillance and human rights... 2016, p. 251; ALLEN, Anita L. Dismantling the "Black Opticon"... 2022, p. 920-921.

Licença *Creative Commons 3.0*

não alcança a violência cotidiana entre estudantes. Uma política de prevenção que concentre seus recursos e sua regulação na vigilância trata a escola como problema de segurança pública, quando os instrumentos capazes de reduzir essa violência pertencem ao campo pedagógico e à proteção integral.

REFERÊNCIAS

ABATE, Constantin. Präventive und repressive Videoüberwachung öffentlicher Plätze. Datenschutz und Datensicherheit, v. 35, n. 7, p. 451-454, 2011.

AGUSTINA, José R.; GALDON CLAVELL, Gemma. The impact of CCTV on fundamental rights and crime prevention strategies: the case of the Catalan Control Commission of Video surveillance Devices. Computer Law & Security Review, v. 27, n. 2, p. 168-174, 2011.

ALLEN, Anita L. Dismantling the "Black Opticon": privacy, race equity, and online data-protection reform. The Yale Law Journal Forum, v. 131, p. 907-958, 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Enunciado CD/ANPD nº 1, de 22 de maio de 2023. Dispõe sobre o tratamento de dados pessoais de crianças e adolescentes. Brasília, 2023.

BERGFINK, Alexander. Videoüberwachung in Fahrzeugen des öffentlichen Personennahverkehrs: Besonderheiten im öffentlichen Personennahverkehr und Prüfung nach deutschem Recht. Datenschutz und Datensicherheit, v. 39, n. 3, p. 145-150, 2015.

BERNAL, Paul. Data gathering, surveillance and human rights: recasting the debate. Journal of Cyber Policy, v. 1, n. 2, p. 243-264, 2016.

BOEHM, Camila. Pesquisa aponta problemas e prisões indevidas a partir do Smart Sampa. Agência Brasil, São Paulo, 4 fev. 2026. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2026-02/pesquisa-aponta-problemas-e-prisoes-indevidas-partir-do-smart-sampa. Acesso em: 18 out. 2026.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília: Presidência da República, 1988.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Diário Oficial da União, Brasília, 11 fev. 2022.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da União, Brasília, 16 jul. 1990.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, 15 ago. 2018.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, v. 81, p. 77-91, 2018.

CÂMARA MUNICIPAL DE SÃO PAULO. Assessoria Jurídica. Parecer ADM nº 035/2019. São Paulo, 2019.

CAMPINAS. Decreto nº 22.759, de 27 de abril de 2023. Institui o Protocolo Égide como Programa Municipal de Prevenção contra a Prática de Atentados Violentos nas Dependências das Escolas Municipais. Campinas, 2023.

CAMPINAS. Decreto nº 24.328, de 5 de março de 2026. Estabelece princípios e parâmetros para a instalação de câmeras de monitoramento circunscritas ao Protocolo Égide, em escolas que integram o sistema municipal de ensino de Campinas, e define procedimentos e atribuições para o tratamento, o uso e a destinação das imagens produzidas. Diário Oficial do Município de Campinas, n. 13.780, 6 mar. 2026.

Licença *Creative Commons 3.0*

CEIA, Vanessa; NOTHWEHR, Benji; WAGNER, Liz. Género y tecnología: un análisis interseccional de las tendencias claves con el enfoque de derechos. Boston: Oxfam America, 2021. (Serie de Investigación de Oxfam).

CITRON, Danielle Keats; SOLOVE, Daniel J. Privacy harms. [S. l.: s. n.], 2021. 55 p. Manuscrito.

GARGIULO, Enrico. Monitoring or selecting? Security in Italy between surveillance, identification and categorisation. In: ORRÙ, Elisa; PORCEDDA, Maria Grazia; WEYDNER-VOLKMANN, Sebastian (ed.). Rethinking surveillance and control: beyond the "security versus privacy" debate. Baden-Baden: Nomos, 2017. p. 195-216.

GARLAND, David. The culture of control: crime and social order in contemporary society. Oxford: Oxford University Press, 2001.

GILL, Martin; SPRIGGS, Angela. Assessing the impact of CCTV. London: Home Office Research, Development and Statistics Directorate, 2005. (Home Office Research Study, 292).

HERRON, Patrick. Beyond balance: targeted sanctions, security and republican freedom. In: ORRÙ, Elisa; PORCEDDA, Maria Grazia; WEYDNER-VOLKMANN, Sebastian (ed.). Rethinking surveillance and control: beyond the "security versus privacy" debate. Baden-Baden: Nomos, 2017. p. 21-48.

HOROWITZ, Sarah. Foucault's Panopticon: a model for NSA surveillance? In: MILLER, Russell A. (ed.). Privacy and power: a transatlantic dialogue in the shadow of the NSA-Affair. Cambridge: Cambridge University Press, 2017. p. 39-62.

LYON, David. Surveillance, security and social sorting: emerging research priorities. International Criminal Justice Review, v. 17, n. 3, p. 161-170, 2007.

MATTSSON, Christer; SÄLJÖ, Roger. Violent extremism, national security and prevention: institutional discourses and their implications for schooling. British Journal of Educational Studies, v. 66, n. 1, p. 109-125, 2018. DOI: 10.1080/00071005.2017.1337870.

MELLO, Daniel. SP abre central de vigilância de câmeras com reconhecimento facial. Agência Brasil, São Paulo, 4 jul. 2024. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2024-07/sp-abre-central-de-vigilancia-de-cameras-com-reconhecimento-facial. Acesso em: 18 out. 2026.

MONAGREDA, Johanna K. Por que falar de raça quando falamos de dados pessoais, inteligência artificial e algoritmos? In: GONÇALVES, Adriana; TORRE, Luísa; MELO, Paulo Victor (ed.). Inteligência artificial e algoritmos: desafios e oportunidades para os media. Covilhã: LabCom, 2024. p. 103-133.

MORAIS, Larissa de. Escolas de Campinas terão reconhecimento facial? Entenda PL. ACidade ON Campinas, Campinas, 7 out. 2026. Disponível em: https://www.acidadeon.com/campinas/politica/escolas-de-campinas-terao-reconhecimento-facial-entenda-pl/. Acesso em: 18 out. 2026.

NGUYEN, Alexander. Videoüberwachung in sensitiven Bereichen: die Zulässigkeit der Beobachtung sensitiver Daten nach deutschem und europäischem Recht. Datenschutz und Datensicherheit, v. 35, n. 10, p. 715-717, 2011.

OLIVEIRA, Samuel R. de. Sorria, você está sendo filmado!: repensando direitos na era do reconhecimento facial. São Paulo: Thomson Reuters Brasil, 2020. E-book.

ORRÙ, Elisa; PORCEDDA, Maria Grazia; WEYDNER-VOLKMANN, Sebastian. Introduction. In: ORRÙ, Elisa; PORCEDDA, Maria Grazia; WEYDNER-VOLKMANN, Sebastian (ed.). Rethinking surveillance and control: beyond the "security versus privacy" debate. Baden-Baden: Nomos, 2017. p. 11-20.

PESCI, Helio de Souza. Avaliação da implementação e execução do Protocolo Égide no âmbito das escolas municipais de Campinas (SP). 2026. Dissertação (Mestrado em Educação) – Pontifícia Universidade Católica de Campinas, Campinas, 2026.

Licença *Creative Commons 3.0*

PIZA, Eric L.; WELSH, Brandon C.; FARRINGTON, David P.; THOMAS, Amanda L. CCTV surveillance for crime prevention: a 40-year systematic review with meta-analysis. Criminology & Public Policy, v. 18, n. 1, p. 134-159, 2019.

PORCEDDA, Maria Grazia. The recrudescence of 'security v. privacy' after the 2015 terrorist attacks, and the value of 'privacy rights' in the European Union. In: ORRÙ, Elisa; PORCEDDA, Maria Grazia; WEYDNER-VOLKMANN, Sebastian (ed.). Rethinking surveillance and control: beyond the "security versus privacy" debate. Baden-Baden: Nomos, 2017. p. 137-180.

QUEIROZ, Christina. Disseminação de discursos de ódio agrava violência escolar. Revista Pesquisa FAPESP, São Paulo, n. 350, abr. 2025. Disponível em: https://revistapesquisa.fapesp.br/disseminacao-de-discursos-de-odio-agrava-violencia-escolar/. Acesso em: 18 out. 2026.

RATCLIFFE, Jerry H.; ROSENTHAL, Jessica M. Video surveillance of public places. 2. ed. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services, 2021. (Problem-Oriented Guides for Police. Response Guide Series, n. 4).

REDE DE OBSERVATÓRIOS DA SEGURANÇA. Retratos da violência: cinco meses de monitoramento, análises e descobertas. Rio de Janeiro: Centro de Estudos de Segurança e Cidadania, 2019.

SANTOS, Ana Luiza; JACOBS, Edgar. Instalação de câmeras de segurança em instituições de ensino é considerada constitucional pelo TJSP. Jacobs Consultoria, 26 abr. 2022. Disponível em: https://www.jacobsconsultoria.com.br/post/instala%C3%A7%C3%A3o-de-c%C3%A2meras-de-seguran%C3%A7a-em-institui%C3%A7%C3%B5es-de-ensino-%C3%A9-considerada-constitucional-pelo-tjsp. Acesso em: 18 out. 2026.

SÃO JOSÉ DO RIO PRETO. Lei nº 12.953, de 2018. Dispõe sobre a instalação de câmeras de monitoramento de segurança nas creches e escolas públicas municipais. São José do Rio Preto, 2018.

SÃO PAULO (Município). Decreto nº 63.552, de 4 de julho de 2024. Institui o Programa Smart Sampa. Diário Oficial da Cidade de São Paulo, São Paulo, 2024.

SÃO PAULO (Município). Secretaria Municipal de Educação; Secretaria Municipal de Segurança Urbana. Portaria Conjunta SME/SMSU nº 4, de 12 de dezembro de 2024. Dispõe sobre o funcionamento do Programa Smart Sampa no âmbito da Secretaria Municipal de Educação. Diário Oficial da Cidade de São Paulo, São Paulo, 2024.

SÃO PAULO (Município). Smart Sampa chega a 50 mil câmeras e já supera em 25% o previsto no Programa de Metas. São Paulo: Prefeitura de São Paulo, 1 abr. 2026. Disponível em: https://prefeitura.sp.gov.br/web/seguranca_urbana/w/smart-sampa-chega-a-50-mil-c%C3%A2meras-e-j%C3%A1-supera-em-25-o-previsto-no-programa-de-metas. Acesso em: 18 out. 2026.

SCHMIDT, Nico; COELHO, Leonardo. 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: 18 out. 2026.

SCHNEIER, Bruce. Beyond fear: thinking sensibly about security in an uncertain world. New York: Copernicus Books, 2003.

SEIFERT, Bernd. Videoüberwachung im künftigen Beschäftigtendatenschutzrecht: was bleibt, was geht, was kommt? Datenschutz und Datensicherheit, v. 35, n. 2, p. 98-108, 2011.

SPOSITO, Marilia Pontes. Um breve balanço da pesquisa sobre violência escolar no Brasil. Educação e Pesquisa, São Paulo, v. 27, n. 1, p. 87-103, jan./jun. 2001.

TAYLOR, Emmeline. I spy with my little eye: the use of CCTV in schools and the impact on privacy. The Sociological Review, v. 58, n. 3, p. 381-405, 2010.

TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. Mantida lei sobre instalação de câmeras em escolas de Rio Preto. São Paulo, 28 set. 2018. Disponível em: https://www.tjsp.jus.br/Noticias/Noticia?codigoNoticia=53595&pagina=1. Acesso em: 18 out. 2026.

Licença *Creative Commons 3.0*

Data de Recebimento: 22/10/2026.
Data de Aprovação: 05/11/2026.

Licença *Creative Commons 3.0*