XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

DANIELLE JACON AYRES PINTO

GUSTAVO RABAY GUERRA

JOSÉ RENATO GAZIERO CELLA

JÉSSICA FACHIN

I61

Internet: dinâmicas da segurança pública internacional[Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto, Gustavo Rabay Guerra, José Renato Gaziero Cella, Jéssica Fachin – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-285-8
Modo de acesso: www.conpedi.org.br em publicações
Tema: Os Caminhos Da Internacionalização E O Futuro Do Direito

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Internet. 3. Segurança pública internacional. XXXII Congresso Nacional do CONPEDI São Paulo - SP (4: 2025: Florianópolis, Brasil).

CDU: 34

XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

Apresentação

No XXII Congresso Nacional do CONPEDI, realizado nos dias 26, 27 e 28 de novembro de 2025, o Grupo de Trabalho - GT “Internet: Dinâmicas da Segurança Pública e Internacional”, que teve lugar na tarde de 28 de novembro de 2025, destacou-se no evento não apenas pela qualidade dos trabalhos apresentados, mas pelos autores dos artigos, que são professores pesquisadores acompanhados de seus alunos pós-graduandos. Foram apresentados artigos objeto de um intenso debate presidido pelos coordenadores.

Esse fato demonstra a inquietude que os temas debatidos despertam na seara jurídica. Cientes desse fato, os programas de pós-graduação em direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao direito. Para apresentar e discutir os trabalhos produzidos sob essa perspectiva.

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema “Internet: Dinâmicas da Segurança Pública e Internacional”. Trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em direito, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores

Prof. Dr. José Renato Gaziero Cella

Prof. Dra. Danielle Jacon Ayres Pinto

Prof. Dr. Gustavo Rabay Guerra

Prof. Dra. Jéssica Fachin

SISTEMAS DE SEGURANÇA E MONITORAMENTO: UM DESCONFORTO NECESSÁRIO?

SECURITY AND SURVEILLENCE SISTEMS: A NECESSARY DISCONFORT?

Juliana Mattos Dos Santos Joaquim [1]

Resumo

O presente trabalho analisa criticamente o uso de tecnologias de vigilância urbana com ênfase nos sistemas de reconhecimento facial, abordando seus impactos sobre direitos fundamentais como a privacidade, a proteção de dados e a autodeterminação informativa. Partindo da evolução histórica da busca por segurança, o estudo destaca como, na contemporaneidade, essa necessidade passou a justificar práticas de vigilância opaca, automatizada e muitas vezes desprovida de regulamentação eficaz. Fundamentado em pesquisa bibliográfica e documental, com foco em casos brasileiros recentes, o artigo examina a assimetria entre a promessa de segurança e os riscos de violação de direitos, sobretudo diante da coleta de dados biométricos sensíveis sem consentimento. A análise inclui falhas técnicas, discriminações algorítmicas e ausência de accountability nas parcerias público-privadas. Conclui-se que a atual arquitetura de vigilância urbana carece de uma regulação robusta, transparente e constitucionalmente orientada, sob risco de aprofundar desigualdades e violar garantias individuais. Defende-se, por fim, a construção de um marco legal específico que assegure o uso ético e proporcional dessas tecnologias, preservando a dignidade humana e princípios constitucionais fundamentais em meio aos avanços tecnológicos.

Palavras-chave: Vigilância algorítmica, Reconhecimento facial, Privacidade, Proteção de dados, Capitalismo de vigilância

Abstract/Resumen/Résumé

This paper critically analyzes the use of urban surveillance technologies, with an emphasis on facial recognition systems, addressing their impact on fundamental rights such as privacy, data protection, and informational self-determination. Based on the historical evolution of the human pursuit of security, the study highlights how, in contemporary times, this need has come to justify opaque and automated surveillance practices, often lacking effective regulation. Grounded in bibliographic and documentary research, with a focus on recent Brazilian cases, the article examines the asymmetry between the promise of security and the risks of rights violations, especially in the collection of sensitive biometric data without consent. The analysis includes technical failures, algorithmic discrimination, and a lack of accountability in public-private partnerships. It concludes that the current architecture of

[1] Doutoranda em Direito pela Universidade Federal Fluminense (PPGD/UFF). Mestre em Direito e Políticas Públicas pela UNIRIO. Membro da Comissão de Proteção de dados e Privacidade da OAB/RJ. Pesquisadora e Advogada.

urban surveillance lacks robust, transparent, and constitutionally guided regulation, posing a risk of deepening inequalities and violating individual guarantees. The paper ultimately advocates for the development of a specific legal framework to ensure the ethical and proportional use of these technologies, preserving human dignity and fundamental constitutional principles amid technological advancements.

Keywords/Palabras-claves/Mots-clés: Algorithmic surveillance, Facial recognition, Privacy, Data protection, Surveillance capitalism

1. INTRODUÇÃO

Por ser característico de sua essência, a busca pela segurança, de si e das suas posses, sempre acompanhou a história humana desde suas primeiras organizações sociais. Além de instintivo, faz parte da cadeia de necessidades estruturais apontada por Maslow ocupando o nível básico da hierarquia das necessidades, estando logo após as necessidades fisiológicas como alimentação e respiração. Inicialmente, isso significava buscar abrigo contra as intempéries climáticas e predadores, passando a necessidade de proteger propriedades, direitos e indivíduos.

À medida que a sociedade humana evolui, os sistemas de segurança também avançam, adaptando-se às mudanças sociais, tecnológicas e econômicas. Na antiguidade, grandes muralhas protegiam cidades contra invasões e saqueadores. Hoje, vemos sistemas de monitoramento sofisticados e em tempo real, integrados com agentes públicos.

Com o surgimento das cidades, após um longo processo de evolução das civilizações de nômades para sociedades urbanas, a necessidade de segurança ganhou novas dimensões. No ambiente urbano, isso impulsionou o desenvolvimento de tecnologias de vigilância cada vez mais avançadas, especialmente aquelas baseadas em reconhecimento facial. Este trabalho propõe uma reflexão crítica sobre os impactos sociais, éticos e jurídicos do uso das tecnologias de vigilância, problematizando o discurso da segurança pública frente aos direitos fundamentais. A partir de uma abordagem qualitativa e bibliográfica, com base em documentos, relatórios e estudos de caso brasileiros, especialmente a partir de 2019, pretende-se discutir os limites da vigilância algorítmica, considerando a opacidade dos sistemas de monitoramento – alguns de iniciativa privada – e o risco de violações de privacidade e autodeterminação informativa. O estudo adota uma abordagem qualitativa, de caráter descritivo-analítico, fundamentada em pesquisa bibliográfica e documental, com ênfase em casos brasileiros recentes, centrando-se no período pós-2019, quando se intensificaram as iniciativas públicas voltadas ao uso de tecnologias de monitoramento urbano com reconhecimento facial.

Inicialmente, observamos a instalação de totens de segurança pela iniciativa privada nas grandes cidades, seguida da adoção da mesma tecnologia pelos órgãos públicos, seja por meio de parcerias que envolvem o fornecimento das imagens e dados coletados a pedido do ente público, seja pela implementação de sistemas próprios de monitoramento, como a Central de Inteligência, Vigilância e Tecnologia em Apoio à Segurança Pública – *Civitas*, no Rio de Janeiro. A partir dessa evolução, e realizando uma análise crítica, buscamos refletir sobre as implicações dessas tecnologias para os direitos fundamentais, como a privacidade e a

autodeterminação informativa, levando em consideração a opacidade dos sistemas algorítmicos e os riscos de violações desses direitos. Ao integrar uma análise das transformações tecnológicas com uma reflexão sobre os desafios éticos e jurídicos decorrentes do uso dessas ferramentas, o estudo pretende contribuir para o debate sobre a proteção dos direitos individuais diante das inovações tecnológicas no campo da segurança pública.

2. A vigilância

Antes de iniciarmos qualquer estudo sobre as consequências da vigilância – estatal ou privada - como fonte de coleta de dados, precisamos observar estudos já realizados por autores que anteriormente já questionavam seu viés controlador ou deturpado, ou seja, desassociado do conceito de proteção que víamos nos primeiros moldes organizacionais sociais.

Em autores como Zygmunt Bauman e Michel Foucault conseguimos compreender que a vigilância é instrumento essencial de controle social. Para Foucault, o poder de vigilância reforça o desequilíbrio entre quem observa e quem é observado, e nesta concepção teríamos o exercício de um poder que busca produzir saber a respeito dos vigiados e adestrar os seus comportamentos. Essa lógica se intensifica na contemporaneidade, especialmente com os mecanismos de segurança que coletam dados continuamente sob a justificativa de interesse público. Nesse contexto, a vigilância não apenas registra, mas molda comportamentos e estrutura formas de controle institucionalizadas.

Complementarmente, o conceito de capitalismo de vigilância, proposto por Shoshana Zuboff (2019), revela como a coleta massiva de dados passou a servir interesses econômicos, tornando-se um fim em si mesma. Frank Pasquale (2015) contribui ao alertar para a opacidade dos sistemas algorítmicos — verdadeiras caixas pretas algorítmicas que dificultam a fiscalização e a responsabilização. No Brasil, autores como Ceia e Teffé (2022) e Azevedo et al. (2022) discutem os impactos dessas tecnologias no campo dos direitos fundamentais, apoiados por estudos institucionais como os do LAPIN (2021) e da Europol (2025).

Como destaca Bauman (2014, p. 109), a ânsia humana reside na busca por um habitat que não gere problemas ou preocupações — uma incessante procura por conforto e conveniência. À luz dessa compreensão, e observando a pirâmide de Maslow[1], percebe-se que

[1] O autor em sua Teoria da Hierarquia das Necessidades Humanas, estabelece níveis hierárquicos das necessidades humanas, onde os humanos realizam escolhas comportamentais com base nas suas necessidades pessoais. O autor organiza as necessidades humanas em cinco níveis, dispostos de forma hierárquica — da base ao topo — conforme a ordem em que tendem a ser buscadas. Na base estão as necessidades fisiológicas, como respiração, alimentação, sono e excreção, fundamentais para a sobrevivência. Em seguida, surgem as necessidades de segurança, que

a humanidade interage com o meio ambiente, prioritariamente, para suprir necessidades básicas como alimentação, segurança e abrigo. Com o crescimento desordenado das cidades, essa necessidade por segurança foi intensificada. Evoluímos das tecnologias bélicas utilizadas para monitoramento de foguetes balísticos (Oliveira, 2021, p. 39) para sofisticados sistemas de vigilância por câmeras, incluindo ferramentas como o reconhecimento facial. Trata-se de um salto na evolução humana que atravessa diferentes contextos históricos: da Revolução Industrial e suas máquinas, ao uso da eletricidade e produção em série da Segunda Revolução Industrial, passando pela automação e digitalização da Terceira Revolução e a contemporânea Quarta Revolução Industrial, marcada pela integração de tecnologias digitais, físicas e biológicas, como inteligência artificial, internet das coisas e uso massivo de dados.

Vemos, portanto, que a discussão não é escassa em um mundo de excessos: de coleta de dados, de totens de segurança, de falhas de acurácia. E desta forma, no escopo deste estudo, propomos observar os sistemas de vigilância urbanos — especialmente os totens interativos de segurança — disseminados em larga escala nas cidades e em espaços públicos[2], e que fazem parte da lógica de vigilância presente no conceito de *surveillance capitalismo* (capitalismo de vigilância) proposto por Shoshana Zuboff, para quem "a vigilância deixou de ser um meio para se tornar um fim comercial em si mesmo" (Zuboff, 2019, p. 12), em suma, um estado de super vigilância questionável. Para a autora capitalismo de vigilância é a reivindicação unilateral da experiência humana privada que é a matéria-prima utilizada para traçar dados comportamentais (Zuboff, 2019).

Tais dispositivos, frequentemente equipados com câmeras, sensores de áudio, reconhecimento facial, botões de emergência e conexão em tempo real com centrais de monitoramento, operam como instrumentos de vigilância contínua da população sob a justificativa de segurança pública. E neste ponto que apresentamos a discussão central do estudo, já que pode inexistir transparência quanto ao seu uso e à destinação dessas informações, sem descartar a possibilidade de danos causados por um reconhecimento falho, por falhas de acurácia[3].

---

envolvem proteção do corpo, estabilidade no emprego, saúde, recursos e propriedade. No terceiro nível, aparecem as necessidades sociais, como amizade, vínculos familiares e intimidade. A quarta camada refere-se à estima, incluindo autoestima, confiança, respeito próprio e reconhecimento social. No topo da pirâmide está a autorrealização, que contempla moralidade, criatividade, espontaneidade, ausência de preconceitos e aceitação dos fatos. A teoria propõe que as necessidades superiores só se tornam prioritárias quando as inferiores estão suficientemente atendidas.

[2] Há que se diferenciar dos sistemas de segurança e monitoramento particulares encontrados em condomínios ou comércios, e que são utilizados como sistema de segurança interno. Diferente dos aqui estudados, que são instalados em locais públicos – nos espaços externos.

[3] Nível de exatidão dos resultados obtidos pela aplicação de tecnologia.

3. Privacidade, proteção de dados e suas assimetrias:

Precisamos, antes de falar sobre privacidade, observar outro conceito fundante que o precede, posto que não há como falar deste sem observar antecipadamente o que nos traz as duas vertentes da liberdade. Neste tópico portanto temos dois direcionamentos para a liberdade, como menciona Isaiah Berlin, em *Dois Conceitos de Liberdade*, este princípio se distingue entre liberdade negativa e liberdade positiva, e é partindo desta diferenciação, ou melhor dizendo, conceituação que iremos compreender a privacidade aqui proposta.

A liberdade negativa diz respeito à ausência de interferência externa: sou livre na medida em que ninguém me impede de agir como desejo, dentro de uma esfera mínima de autonomia individual. Já a liberdade positiva refere-se à autodeterminação, ou seja, ao poder de ser senhor de si mesmo e conduzir a própria vida com base na razão. Enquanto a primeira está ligada à proteção contra coerções alheias, a segunda pode justificar, paradoxalmente, intervenções autoritárias sob o argumento de "libertar" alguém de sua ignorância ou irracionalidade. Berlin alerta que, ao tentar definir o "verdadeiro eu" de alguém, corre-se o risco de oprimir em nome de uma suposta liberdade. Em seu diálogo, questiona 'Quem me governa?' 'sou meu próprio mestre?' ao diferenciar a liberdade negativa da positiva quando indaga 'Quão longe o governo interfere comigo?'. Para o autor, é nessa diferença que encontramos contraste entre os dois conceitos de liberdade (negativa e positiva).

Tal diferenciação é importante para entendermos o direito a privacidade ou o desrespeito a ela quando da utilização de sistemas de monitoramento neste trabalho discutidos. A privacidade neste contesto é liberdade negativa, ou seja, o Estado não pode invadir a esfera de proteção que este direito cria ao redor de seu titular, gerando a este o poder de reivindicar, frente à autoridade pública, a proteção contra a violação deste direito por terceiros ou pelo próprio Poder Público.

A privacidade, como visto: uma liberdade negativa, ou seja, direito que não permite interferência Estatal na vida privada – senão em virtude de lei – é direito fundamental presente em nosso regimento Constitucional, na Declaração dos Direitos Humanos e em muitas outras passagens legais presentes em nosso ordenamento[4]. Já a Proteção de dados, uma liberdade

[4] Referimo-nos ao Art. 5, inciso X da Constituição de 1988: **X** - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação e Art. 12 Declaração dos Direitos Humanos: Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra intromissões ou ataques toda a pessoa tem direito a proteção da lei. Já no Codigo Civil, vemos nos Art. 11 ao 21.

positiva[5], exige atuação Estatal, com sua regulamentação e fiscalização – inclusive para evitar ferir direitos fundamentais tais como a privacidade – tal direito fundamental originário do direito à privacidade pode ser observado no texto constitucional no Art. 5 LXXIX[6].

Podemos dizer, portanto, que ambos os direitos fundamentais estão profundamente ligados, embora sejam distintos em sua essência. Desta forma o direito à privacidade com sua origem constitucional tem como finalidade a proteção dos aspectos essenciais da vida pessoal, como a intimidade e o sigilo das comunicações, restringindo a intervenção do Estado àquelas situações de necessidade legalmente justificadas. Nesse mesmo sentido, a Lei Geral de Proteção de Dados (LGPD) surge como instrumento normativo voltado à tutela dos dados pessoais — comuns ou sensíveis — diante da crescente necessidade de resguardar os cidadãos contra o uso indevido de suas informações por agentes públicos e privados, fortalecida pela previsão agora constitucional após a emenda 115/2022[7].

Esta investida, que levou demasiado tempo para se instalar, vide o lapso temporal entre a LGPD, Lei 13.709/2018 e a Emenda 115/2022 se justifica diante das mudanças que as novas Tecnologias da Informação e da Comunicação impuseram à sociedade (intensificada após a pandemia de 2019 com a massificação da transferencia de dados e automação das relações sociais), especialmente no tratamento de dados pessoais pelo Estado e pelas empresas privadas, exigindo a consolidação de um direito à proteção de dados pessoais para proteger aspectos da personalidade humana.

É inegável que toda a conquista humana, traduzida em avanços tecnológicos acabaram modificando significativamente a forma como a esfera pública e privada administravam as informações coletadas dos cidadãos, e passou a não caber mais toda essa dinâmica em um único conceito como o de privacidade que já possuia seus preceitos bem delineados. Da mesma forma não podemos conceber retrocesso no desenvolvimento humano e tecnológico[8], não é admissível estagnar os preceitos legais protetores de direitos já instituídos.

---

[5] A privacidade assume seu conceito positivo, ao reivindicar autodeterminação informativa, garantindo ao indivíduo o poder de decidir sobre seus próprios dados e sobre como sua vida será exposta permitindo que o titular controle o acesso à sua esfera privada, como exemplifica a LGPD, ao assegurar o direito de consentir — ou não — com o uso de suas informações.

[6] É assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022)

[7] Precisamos ter consciência que existem Estados constitucionais onde um direito fundamental à proteção.de dados não é reconhecido. A Emenda Constitucional nº 115/2022 marcou um avanço ao reconhecer a **proteção de dados pessoais como direito fundamental autônomo** no Brasil. O que víamos de forma tímida no inciso LXXIX do artigo 5º da Constituição com a Emenda, conferiu proteção material e formal, dando status de cláusula pétrea constitucional, bem como garantindo eficácia imediata.

[8] Para Dhiego de Almeida (p. 225,2022), tais mudanças observadas no setor público e privado ocorreram no contexto da transição das sociedade pós-industrial para a da informação. A informação passou a ser o elemento

Em síntese, a relação simbiótica entre privacidade e proteção de dados pessoais tem se mostrado insuficiente diante da complexidade informacional da sociedade contemporânea, e por este motivo a consideramos assimétricas. Nos parece que ao realizar capitação, manipulação e guarda de dados, estamos imediatamente desrespeitando a noção de privacidade. Isso pois o contesto da privacidade estaria relacionado ao controle de informações íntimas ou privadas, enquanto a proteção de dados pessoais ultrapassa esse recorte, por abranger informações acessíveis publicamente, nas quais o foco pode recair sobre aspectos como a exatidão dos dados. Assim, a qualificação da proteção de dados como direito da personalidade, e não somente uma mera continuidade do direito a privacidade, contribui para uma interpretação mais coerente, viabilizando levantar prerrogativas como o direito de retificação e o direito à revisão de decisões automatizadas.

Nessa linha, Dhiego Melo Job de Almeida (2022, p. 230) sustenta que, além de se consolidar como direito da personalidade autônomo, o direito à proteção de dados pessoais também pode ser compreendido como um direito fundamental implícito, o que fortalece sua autonomia normativa frente ao direito à privacidade.

É diante deste contexto que a diferenciação entre privacidade e proteção de dados se revela ainda mais crucial, e vista do crescimento exponencial do uso de tecnologias de monitoramento por câmeras de segurança e vigilância biométrica, tanto por gerenciamento público quanto privado é fundamental ter o entendimento de que esses mecanismos, podem promover segurança e eficiência, mas também ampliar os riscos de exposição indevida, discriminação algorítmica e violação da dignidade humana. Assim, há de se reconhecer a proteção de dados como um direito fundamental autônomo e ativo, que exige do Estado não apenas a abstenção de interferência (como no caso da privacidade), mas sobretudo uma atuação normativa, reguladora e fiscalizatória constante, para que o tratamento dessas informações ocorra de forma legítima, e alinhada aos valores constitucionais que visam preservar a liberdade e a identidade dos indivíduos na sociedade digital.

4.2 Vigilância algorítmica e opacidade tecnológica

nuclear ao desenvolvimento econômico sendo o elemento estruturante que organiza a sociedade, papel antes que seria da propriedade.

Já vimos anteriormente que na concepção de Michel Foucault, o poder de vigilância é automático e desindividualizado, consolidando um desequilíbrio estrutural entre observadores e observados. A vigilância permitiria, portanto, a produção de conhecimento sobre aqueles que são vigiados o que se torna um aspecto fundamental para o exercício do controle e do poder.

No caso dos totens urbanos, o cidadão se converte não apenas em alvo de observação, mas em fonte contínua de dados que alimentam sistemas automatizados de controle, configurando um cenário de governança algorítmica que exige limites legais claros.

Contudo, estamos diante de uma situação peculiar e antagônica: Durante todo o seu processo evolutivo, a humanidade buscou por segurança, seja nas muralhas de um castelo, ou em cidades altamente tecnológicas e com monitoramento contínuo. E obviamente as torres do vigia foram substituídas por tecnologia de vigilância cotidiana em prol do benefício coletivo. Contudo, se por um lado oferecem sensação de segurança e resposta rápida a emergências, por outro suscitam questionamentos relevantes sobre privacidade, tratamento de dados pessoais e controle social invisível.

O que observamos na atualidade é um modelo de vigilância urbana descentralizada e automatizada, característico das *smart city*, e que exige especial atenção quanto à transparência algorítmica, responsabilização institucional e respeito aos direitos fundamentais dos cidadãos, pois ao passo que vigia, molda comportamentos e produz efeitos sobre as liberdades individuais, especialmente quando associada a tecnologias opacas, como o reconhecimento facial, ponto que veremos mais adiante.

Tal tecnologia, baseada em um conjunto de instrumentos digitais voltados à verificação e identificação automatizada de rostos humanos, pode ser classificada de acordo com suas finalidades específicas, como autenticação, vigilância ou monitoramento comportamental. Forma de biometria automatizada, que emprega algoritmos avançados para detectar e analisar padrões faciais a partir de dados captados em tempo real. No entanto, à semelhança do que ocorre com a coleta massiva de dados em redes sociais — potencializada pelo uso de inteligência artificial —, o funcionamento desses sistemas — muitas vezes opaco e análogo a uma “caixa-preta algorítmica” (Pasquale, 2015, p. 3), suscita relevantes controvérsias jurídicas, éticas e sociais, especialmente no que diz respeito à transparência, à responsabilização e à proteção dos direitos fundamentais.

Observando por esta ótica, e sabendo da opacidade destes sistemas, a onipresença do Estado, sob o pretexto de garantir a segurança coletiva, torna-se perigosa quando seus mecanismos são utilizados por ou para fins duvidosos. Como nas distopias orwellianas, os "olhos que tudo veem" não apenas observam, mas interconectam dados que tendem a ser

utilizados para diversos propósitos. Isso pode acarretar graves riscos aos direitos fundamentais, sobretudo se tais informações forem empregadas abusivamente para exercer controle político e social (CEIA e TEFFÉ, 2022, p. 197).

4.3 Reconhecimento facial e a violação de direitos fundamentais

Outro aspecto crítico relacionado ao uso da tecnologia de reconhecimento facial refere-se ao seu nível de precisão. A falta de acurácia desses sistemas — manifestada tanto na identificação equivocada de indivíduos inocentes quanto na falha em reconhecer pessoas efetivamente procuradas — pode gerar consequências graves, especialmente quando seu uso está inserido no contexto da segurança pública. Tais falhas se tornam ainda mais problemáticas, pois comprometem diretamente os direitos e garantias individuais. Observa-se, de forma recorrente, erros de identificação que resultam na abordagem e detenção de cidadãos inocentes, exigindo destes a demonstração de sua inocência perante o Estado.

No Brasil, a utilização desta tecnologia se intensificou após 2014, com o monitoramento de grandes eventos como a Copa do Mundo ou Olimpíadas (2016) se consolidando com a Portaria nº 793/2019[9] (DPU, 2025) sem qualquer tipo de regulação mais direcionada, eficaz e que resguardasse direitos fundamentais e com a finalidade de garantir transparência. O que torna ainda mais preocupante as suas falhas técnicas nos reconhecimentos, o algorítmico se mostra tendencioso, de forma a apresentar taxas de erro elevadas para determinados grupos populacionais, visto que sua taxa de erro se mostra desproporcional na relação entre pessoas negras, indígenas e asiáticas quando comparadas com pessoas brancas.

Se analisarmos a situação em território brasileiro, os dados refletem que as abordagens policiais, em inúmeras oportunidades se basearam em identificação facial equivocada (Nunes, p. 5, 2025). De acordo com o Relatório de Mapeando a Vigilância Biométrica elaborado pela Defensoria Pública da União (DPU) e o Centro de Estudos de Segurança e Cidadania (CESeC) evidência como a falta de acurácia dos sistemas de reconhecimento facial pode comprometer gravemente os direitos fundamentais dos cidadãos. Não falamos apenas, neste momento, da

[9] Art. 4º O Eixo Enfrentamento à Criminalidade Violenta compreende o conjunto de medidas para redução e controle da violência e da criminalidade, a serem desenvolvidas em territórios que apresentam altos indicadores criminais, ampliando a percepção de segurança e proteção social, por meio de ações multidisciplinares, intersetoriais e de integração de atores nas diversas esferas. § 1º O Eixo a que se refere o caput será composto pelas seguintes ações: III - reaparelhamento e modernização das instituições de segurança pública, com vistas à prevenção ou à repressão qualificada e à redução da criminalidade violenta e de enfrentamento ao crime organizado, com destaque para as seguintes linhas de atuação: b) fomento à implantação de sistemas de videomonitoramento com soluções de reconhecimento facial, por Optical Character Recognition - OCR, uso de inteligência artificial ou outros;

falta de transparência[10], um dos pontos destacados pelo relatório como ponto crítico, mas das falhas de reconhecimento.

Em 2019, no Rio de Janeiro, uma mulher inocente foi detida após ser erroneamente identificada pelo sistema como autora de crimes. Posteriormente, constatou-se que a verdadeira suspeita já estava presa desde 2015, mas, mesmo assim, permanecia no banco de dados como procurada, evidenciando falhas tanto no sistema de identificação quanto na gestão da base de dados (Correio, 2019). De forma semelhante, o relatório da organização britânica *Big Brother Watch* revelou que 95% das correspondências realizadas por reconhecimento facial no Reino Unido resultaram em falsos positivos, ou seja, identificações erradas de pessoas inocentes. A entidade destacou que, mesmo com o descarte das imagens sem correspondência, o armazenamento dos rostos reconhecidos erroneamente contraria os princípios da finalidade e necessidade previstos nas legislações de proteção de dados (BBW, 2018).

Mais recentemente, em dezembro de 2024, o sistema *Smart Sampa*, da Prefeitura de São Paulo, confundiu um aposentado de 80 anos com um estuprador foragido. Francisco Ferreira da Silva, voluntário em uma unidade básica de saúde, foi abordado por agentes da Guarda Civil Metropolitana e levado à delegacia, onde permaneceu por cerca de dez horas, mesmo sem qualquer correspondência de nome ou dados pessoais com o suspeito. Segundo a família, a única semelhança entre os dois seria o aspecto físico superficial — sendo que até a cor da pele diferia. Apesar da nota oficial da Secretaria Municipal de Segurança Urbana afirmar que o sistema é eficiente, o episódio levanta preocupações legítimas quanto à efetividade, segurança e justiça na aplicação dessas tecnologias em políticas públicas de segurança (UOL, 2025).

Na mesma cidade, anos antes um sistema de monitoramento instalado na rede de Metro previa a possibilidade de armazenamento e compartilhamento de imagens dos usuários sem prever a sua destinação ou utilização destes dados coletados, ferindo qualquer princípio de transparência e privacidade. O fato virou algo de Ação Civil Pública (Processo nº: 1010667-97.2022.8.26.0053) movida pela Defensoria Pública do Estado de São Paulo contra a Companhia do Metropolitano de São Paulo, e em acertada decisão da magistrada, determinou

[10] O relatório destaca coo ponto crítico a falta de transparecias na coleta de dados. Segundo o estudo a ausência de informações claras, sobre o uso da tecnologia de reconhecimento facial por parte dos estados seria um obstáculo no controle social, dificultando a prestação de contas e comprometendo a confiança pública, alem de violar princípios constitucionais da publicidade e do acesso à informação. Para tal obstáculo, a pesquisa propõe: elaboração de projeto de lei que tenha como escopo vedações, limites e regras para o uso de tecnologias de reconhecimento facial para fins de segurança pública, bem como estabelecer limites que priorizem a proteção de direitos fundamentais. Chega a destacar a necessidade de suspender o uso das tecnologias de reconhecimento facial (TRF) para fins de segurança pública até que o advento regulamentação específica.

que as tecnologias de reconhecimento e tratamento de dados biométricos usadas pelo sistema não fossem utilizadas. Em sua justificativa estaria o fato de inexistir nos documentos do edital de contratação da empresa responsável pelo sistema qualquer informação sobre os critérios, condições e propósitos da implementação do sistema de reconhecimento facial. Não existiria segundo o ato decisório, informações precisas sobre o armazenamento das informações e utilização do sistema de reconhecimento pessoal, a falta destes quesitos poria em risco direitos fundamentais dos cidadãos além de não atender aos requisitos previstos na Lei Geral de Proteção de Dados (LGPD), no Código de Defesa do Consumidor, no Código de Usuários de Serviços Públicos, no Estatuto da Criança e do Adolescente, na Constituição Federal e nos tratados internacionais.

Outro exemplo que pode ser trazido ao debate está relacionado aos totens de segurança privada que podem ser observados em várias cidades, e que prometem trazer a segurança necessária para uma cidade complexa como a do Rio de Janeiro. Cidade desfavorecida por dados estatísticos que informam o crescimento nos casos de roubo – a cidadãos e veículos - no ano de 2024 em relação a 2023, totalizando 13,6% (58.574) e 39,0% (30.934), respectivamente (ISP, 2021).

A princípio, o serviço, oferecido a título oneroso, é solicitado por condomínios, centros comerciais ou associações de moradores, com o intuito de fortalecer a proteção deficiente do Estado. Tal tecnologia que contém câmeras com capacidade de vigilância em 360º monitoram por 24hrs em tempo real o local desejado, alem de oferecer a possibilidade de consulta do historico de gravações selecionando dia e horario desejados.

Destacamos algo que ainda precisa ser debatido com mais profundidade: não há em tais contratações clareza a respeito da coleta e armazenamento de dados - muito embora tais empresas afirmem que esses dados não são armazenados ou que não ocorra o reconhecimento facial – muito menos autorização para monitoramento sequenciado ou coleta de dados. Como a contratação é realizada por um condomínio por exemplo, dificilmente – para não dizer inexistente – há autorização pontual daqueles que estarão sob vigilância constante. Os moradores passam a ter um monitoramento contínuo de suas rotinas diárias – incluindo horários de chegada e saida, bem como roteiro cotidiano – sem nenhuma ciencia ou anuência. E neste ponto precisamos observar algumas questões importantes. Uma delas é o banco de dados arquivado. As imagens contendo dia e horários que estes moradores tem o costume de sair de sua casa ou chegar de seu trabalho, o que por si só já seria vigilância desautorizada, permite

traçar toda sua rotina, sem dar a certeza de que estes dados estão de fato seguros ou se serão utilizados posteriormente para que perfis sejam traçados[11].

Outro fato é a possibilidade de "venda" dessas informações: Imaginemos que seguradoras utilizem tais dados para localizar veículos em processo de busca e apreensão, utilizando estes mecanismos extraoficiais para alcançar objetivos processuais. Ou ainda, as mesmas câmeras que podem ser utilizadas para reduzir o feminicídio, podem facilitar o crime, viabilizando por meio de mãos erradas que os agressores monitorem suas vítimas.

Esse cenário evidencia não apenas o risco de violações de direitos fundamentais, mas também suscita um questionamento legítimo: o benefício prometido pela tecnologia é realmente maior do que os prejuízos causados por sua aplicação falha? Sistemas com baixo índice de confiabilidade comprometem a eficácia das políticas públicas de segurança e fragilizam a legitimidade do poder estatal no uso de ferramentas de vigilância baseadas em dados sensíveis.

4.4 Regulação ausente e riscos da governança opaca

Antes mesmo de se considerar a hipótese de falhas técnicas nos sistemas de reconhecimento e análise de dados — que, inclusive, têm resultado em punições equivocadas de forma reiterada — é preciso retomar os princípios da vigilância. Hartzog (2018, apud Oliveira, p. 61) argumenta que a vigilância pode ser compreendida como uma ferramenta de opressão, especialmente quando operada em ambientes de ausência regulatória ou desproporcionalidade de poder, noutras palavras, trata-se de uma ferramenta de opressão em contextos marcados por assimetrias de poder e ausência regulatória.

A opacidade desses sistemas suscita questionamentos essenciais: quais dados estão sendo coletados? Quem os armazena? Qual é o destino dessas imagens? Tais perguntas, segundo Ceia e Teffé (2022, p. 208), permanecem sem resposta, diante da evidente ausência de regulamentação, o que contribui para um estado de vigilância opaca, em que direitos fundamentais como a privacidade e a autodeterminação informativa podem ser continuamente violados sem o devido controle social ou jurídico.

[11] De forma breve por nçao caber neste estudo em específico, o algoritmo tende a traçar um perfil do usuário para dizer o que ele precisa naquele momento, e somente tem esta capacidade após ser alimentado com dados destes usuários. Assim, imaginemos moradores de um condomínio monitorado por um sistema interligado de câmeras espalhados pela cidade, possibilitando o algoritmo traçar as rotas e horários habituais de um indivíduo, e que posteriormente esta coleta de dados faça parte de um banco de dados maior viabilizando identificar gostos, necessidades ou rotinas de forma a então transformar tais informações em estatísticas para segmentar clientes, personalizar ofertas, prever comportamentos futuros e até mesmo identificar riscos.

Não por menos que estudo realizado pelo Laboratório de Políticas Públicas e Internet – LAPIN, realizado em 2021 concluiu que é evidente a falta de transparência e de mecanismos garantidores de proteção de dados e segurança na implementação das tecnologias de vigilância no Brasil (Reis et al., 2021, p. 40), para o relatório, lacuna regulatória seria um dos principais entraves para garantir tal proteção. Isso pois o seu funcionamento depende da coleta de dados biométricos, que na maioria das legislações sobre tratamento de dados são considerados dados sensíveis.

Vale lembrar que o Poder Público em sua atividade vigilante é um agente de tratamento de dados pessoais, ao passo que monitora os indivíduos nas vias públicas ou nos meios de transporte, vide debate anterior a respeito da de Ação Civil Pública (Processo nº: 1010667-97.2022.8.26.0053) movida pela Defensoria Pública do Estado de São Paulo contra a Companhia do Metropolitano de São Paulo.

Além disso, não há qualquer consentimento por parte dos titulares dos dados no momento em que esses dispositivos capturam suas rotinas, expressões faciais, inclinações políticas ou sociais — e até mesmo estados emocionais. A justificativa para a manutenção e ampliação desses sistemas costuma ser a promoção do bem comum, remetendo diretamente à lógica do panóptico.

Contudo, não se pode afirmar com certeza que os dados captados serão utilizados de maneira legítima. Há riscos concretos de invasões, vazamentos e usos indevidos dessas informações, inclusive por entidades paraestatais. As Tecnologias de Reconhecimento Facial (TRFs), por vezes, causam danos severos em razão de erros, ou — quando "funcionam bem" — promovem vigilância em massa (Azevedo et al., 2022, p. 145). Não por acaso, movimentos como “Tire meu rosto da sua mira” vêm ganhando cada vez mais adesão, motivados pelo rastreamento constante, pela supressão do anonimato, pela inibição da liberdade de expressão e pela intensificação da perseguição a grupos historicamente marginalizados (Azevedo et al., 2022, p. 146).

Nesse contexto, é imprescindível analisar com rigor as parcerias firmadas entre entes públicos e a iniciativa privada para a implementação de sistemas de monitoramento que, sob o discurso da segurança, capturam dados biométricos de toda uma população. Tais parcerias, muitas vezes, permitem que o poder público utilize imagens e informações sem o consentimento prévio dos cidadãos. Ainda mais grave é o cenário em que o ente público autoriza o uso dessas tecnologias, com a justificativa de um benefício coletivo, mas, na prática, concede carta branca ao setor privado para explorar esses dados em finalidades mercadológicas, como no treinamento de algoritmos voltados à oferta de produtos e serviços (Azevedo et al., 2022, p. 150).

E podemos ainda ser mais alarmistas, de acordo com Yuval Harari, os donos dos dados serão os donos do futuro (Harari, 2018, p. 102), para ele se quisermos evitar a concentração de toda a riqueza sob o domínio de uma pequena elite, deveríamos pensar fortemente em uma eficiente regulamentação sobre a propriedade dos dados (Harari, 2018, p. 106). Foi assim quando a terra era a riqueza maior, logo após quando os processos produtivos eram sinônimo de prosperidade e da mesma forma será com os dados.

Além dos riscos técnicos, há desafios éticos e legais significativos. A coleta de dados faciais, mesmo em ambientes públicos, envolve informações pessoais sensíveis, o que demanda proteção rigorosa sob os marcos legais da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil e do Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia. O relatório da Europol enfatiza que o uso estatal de dados biométricos deve ser acompanhado de mecanismos eficazes de *accountability*, transparência e consentimento informado, sob pena de violação de direitos fundamentais (EUROPOL, 2025, p. 15).

Com dados de 2025 o projeto O Panóptico elaborado pelo Centro de Estudos de Segurança e Cidadania (CESeC), destaca que existem atualmente mais de trezentos projetos de reconhecimento facial operando no Brasil, e deixa claro que a falta de transparência é a maior preocupação. Informa que alguns Estados, em estágio avançado de implementação de programas de Vigilância Biométrica, embora possuam processos de licitação em andamento, não divulgam informações básicas como dados dos fornecedores, os objetivos, fontes de financiamento (Nunes, 2025), e o tratamento e guarda de tais dados.

O relatório elenca uma lista de problemas para o uso implementação e regulação do tema, tais como: problemas relacionados à transparência a falta de padronização no uso da tecnologia, o descumprimento às normas de proteção de dados, incompatibilidade com princípios administrativos, ausência de supervisão e monitoramento, integração ineficiente com sistemas nacionais, falta de delimitação geográfica e temporal das operações de reconhecimento, falta de critérios para a formação e utilização da lista de procurados.

Ou seja, ao que tudo indica, estaríamos distantes de uma regulamentação e utilização segura dos sistemas de vigilância e monitoramento que utilizam a tecnologia de reconhecimento facial. Deve ser considerado ainda que o treinamento dos algoritmos de reconhecimento facial pode reproduzir vieses algorítmicos, afetando desproporcionalmente certos grupos étnicos, faixas etárias e gêneros, como já demonstrado por diversos estudos. O risco de discriminação algorítmica é latente neste meandro.

Diante desse cenário, o uso de câmeras com reconhecimento facial exige não apenas o desenvolvimento de tecnologias seguras e eficazes, mas também uma regulação jurídica

robusta que assegure o equilíbrio entre segurança pública e os direitos fundamentais à privacidade, igualdade e autodeterminação informativa.

5. CONSIDERAÇÕES FINAIS

O uso de câmeras de monitoramento com tecnologia de reconhecimento facial representa um avanço relevante no campo da segurança pública e da investigação criminal, especialmente por permitir a análise massiva e automatizada de imagens em contextos como aeroportos, fronteiras e centros urbanos. Trabalho que se feito por um humano demandaria tempo, erário e poderia gerar incorreções diante das limitações da espécie. Conforme aponta relatório da Europol, a inteligência artificial tem sido amplamente empregada para acelerar a triagem de imagens e viabilizar a identificação facial de suspeitos a partir de bancos de dados criminais ou registros governamentais (EUROPOL, 2025, p. 32-33).

Verificamos, portanto, que o avanço das tecnologias de vigilância, especialmente aquelas baseadas em reconhecimento facial, marca uma inflexão histórica na forma como o poder público e a iniciativa privada exercem controle sobre o espaço urbano e sobre os corpos que nele circulam. Se por um lado essas ferramentas prometem maior eficiência na segurança pública e no combate à criminalidade, por outro lado, instauram um regime de observação contínua, marcado pela opacidade algorítmica, pela ausência de consentimento e pela fragilização de direitos fundamentais como a privacidade, a proteção de dados e a autodeterminação informativa.

A proposta deste estudo foi verificar que a coleta de dados biométricos sensíveis sem consentimento e a possibilidade de erros graves reforçam a necessidade de revisão crítica de sua adoção pelo poder público. O discurso da segurança, quando dissociado de limites jurídicos, éticos e democráticos, pode justificar práticas tecnicamente sofisticadas, mas profundamente assimétricas em seus efeitos sociais

Reforça-se a urgência de um marco legal específico, que estabeleça limites claros, mecanismos de controle, fiscalização e instrumentos de participação social para garantir que a segurança não seja alcançada à custa da liberdade e da dignidade humana. A arquitetura de vigilância em curso nas cidades brasileiras, com destaque para os totens urbanos e sistemas privados de monitoramento em tempo real, vem sendo implementada sem os necessários parâmetros de transparência, controle social e *accountability*, expondo os cidadãos – em

especial os grupos historicamente vulnerabilizados – a riscos desproporcionais de erro, discriminação e violência institucional.

Conclui-se, portanto, que o futuro da segurança pública – em um cenário de rápida digitalização e expansão da vigilância – deve ser orientado por princípios constitucionais sólidos, especialmente os da dignidade da pessoa humana, da proporcionalidade, da legalidade e da transparência. É urgente a construção de uma regulação robusta, multidisciplinar e participativa, que assegure o equilíbrio entre inovação tecnológica e a preservação das liberdades civis.

Sugere-se, como desdobramento deste estudo, o aprofundamento empírico da percepção da população sobre os mecanismos de vigilância facial, a análise de seus impactos concretos em diferentes grupos sociais, bem como a comparação com modelos regulatórios internacionais que promovem o uso ético e proporcional dessas tecnologias. A proteção de dados não é um entrave ao progresso, mas uma salvaguarda essencial à própria ideia de humanidade em tempos de algoritmos.

REFERÊNCIA BIBLIOGRAFICA

ALMEIDA, Dhiego Melo Job de. Direito à privacidade e à proteção de dados pessoais: repercussões da superação do sigilo como único instrumento de tutela da dignidade humana nas exceções do art. 4º da LGPD. *Revista de Estudos Jurídicos UNESP*, Franca, ano 26, n. 44, p. 221, jul./dez. 2022. Disponível em: https://ojs.franca.unesp.br/index.php/estudosjuridicosunesp/issue/archive. Acesso em: 01 ago. 2025.

AZEVEDO, Cynthia Picolo Gonzaga de; MOREIRA, Horrara; ALCÂNTARA, Rafaela Cavalcanti de; RACHID, Raquel. "Tire Meu Rosto da Sua Mira": em busca do banimento de tecnologias de reconhecimento facial na segurança pública brasileira. In: DUARTE, Daniel Edler; CEIA, Eleonora Mesquita (org.). *Tecnologia, segurança e direitos: os usos e riscos de sistemas de reconhecimento facial no Brasil*. Rio de Janeiro: Konrad Adenauer Stiftung, 2022. p. 143-170.

BERLIN, Isaiah. *Dois conceitos de liberdade*. Tradução de Aline Mesquita. Universidade Federal do ABC (UFABC). Disponível em: https://pt.scribd.com/document/565808291/Dois-Conceitos-de-Liberdade-Isaiah-Berlin. Acesso em: 10 jun. 2025.

BIG BROTHER WATCH – BBW. *Face Off: the lawless growth of facial recognition in UK policing*. Maio 2018. Disponível em: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf. Acesso em: 23 abr. 2025.

BRASIL. *Constituição (1988). Constituição da República Federativa do Brasil*. Brasília, DF: Senado Federal, 1988.

BRASIL. *Lei n. 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União: seção 1*, Brasília, DF, 15 ago. 2018. p. 1.

CEIA, Eleonora Mesquita; TEFFÉ, Chiara Spadaccini de. Reconhecimento facial e segurança pública nas cidades: uma análise crítica na perspectiva das competências federativas e dos direitos fundamentais. In: DUARTE, Daniel Edler; CEIA, Eleonora Mesquita (org.). *Tecnologia, segurança e direitos: os usos e riscos de sistemas de reconhecimento facial no Brasil*. Rio de Janeiro: Konrad Adenauer Stiftung, 2022. p. 197-225.

CORREIO. Inocente é confundida com criminosa por câmera de reconhecimento facial no Rio. *Correio*, Da redação, 11 jul. 2019. Disponível em: https://www.correio24horas.com.br/noticia/nid/inocente-e-confundida-com-criminosa-por-camera-de-reconhecimento-facial-no-rio/. Acesso em: 23 abr. 2025.

EUROPOL. *Biometric vulnerabilities: ensuring future law enforcement preparedness*. The Hague: European Union Agency for Law Enforcement Cooperation, 2025. 96 p. Disponível em: https://www.europol.europa.eu/publications. Acesso em: 24 abr. 2025.

FOUCAULT, Michel. *Vigiar e punir: nascimento da prisão*. Petrópolis: Vozes, 1975.

HARARI, Yuval Noah. *21 lições para o século 21*. Tradução: Paulo Geiger. 1. ed. São Paulo: Companhia das Letras, 2018.

INSTITUTO DE SEGURANÇA PÚBLICA DO ESTADO DO RIO DE JANEIRO (ISP/RJ). *Dossiê criança e adolescente 2021*. Rio de Janeiro: ISP/RJ, 2021. Disponível em: https://www.rj.gov.br/isp/node/1507. Acesso em: 19 jun. 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.

OLIVEIRA, Samuel R. de. *Sorria, você está sendo filmado! Repensando direitos na era do reconhecimento facial*. São Paulo: Revista dos Tribunais, 2021.

PASQUALE, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press, 2015.

REIS, Carolina; ALMEIDA, Eduarda; DA SILVA, Felipe; DOURADO, Fernando. *Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil*. Brasília: Laboratório de Políticas Públicas e Internet (LAPIN), 2021. Disponível em: https://lapin.org.br. Acesso em: 24 abr. 2025.

UOL. Reconhecimento facial de SP confunde idoso com estuprador foragido. *UOL Notícias*, 13 abr. 2025. Disponível em: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2025/04/13/reconhecimento-facial-de-sp-confunde-idoso-com-estuprador-foragido.htm. Acesso em: 23 abr. 2025.

ZUBOFF, Shoshana. *Harvard professor says surveillance capitalism is undermining democracy*. *Harvard Gazette*, 4 mar. 2019. Disponível em:

https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/. Acesso em: 29 jul. 2025.

ZUBOFF, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.