Universidade do Contestado | www.unc.br/periodicos ISSNe: 2358-6125
Profanações revista
UnC

O PARADOXO DA PROTEÇÃO: SEGURANÇA, DIREITOS FUNDAMENTAIS E O AVANÇO DAS POLÍTICAS DE RECONHECIMENTO FACIAL SEM REGULAÇÃO

THE PARADOX OF PROTECTION: SECURITY, FUNDAMENTAL RIGHTS, AND THE ADVANCEMENT OF UNREGULATED FACIAL RECOGNITION POLICIES

Hendrisy Araujo Duarte[1]
Rafael Santos de Olveira[2]

RESUMO

O estudo analisa a regulação de tecnologias de videomonitoramento no Brasil, com foco no uso do reconhecimento facial e suas implicações para a segurança pública e os direitos fundamentais. A pesquisa parte do problema: como o Estado brasileiro pode equilibrar a eficiência tecnológica do reconhecimento facial na segurança pública com a proteção de direitos fundamentais, diante da ausência de regulamentação específica e lacunas em transparência, accountability e governança? Utilizando o método dedutivo e o método bibliográfico, a investigação se fundamenta na perspectiva foucaultiana para analisar o papel ambivalente do Estado, que, ao mesmo tempo em que protege direitos fundamentais, expande seu poder em nome da segurança pública. A ausência de regulamentação específica para o reconhecimento facial expõe práticas discriminatórias, alimentadas por vieses algorítmicos e pela apropriação de dados pela iniciativa privada, desafiando os princípios democráticos. A governança, pautada na

[1] Mestra em Direito (UFSM). Mestranda em Políticas Públicas (UNIPAMPA). Pesquisadora do Grupo de Pesquisa em Gênero, Ética, Educação e Política (GEEP/UNIPAMPA) e do Centro de Estudos e Pesquisas em Direito e Internet (CEPEDI/UFSM). Especialista em Direito Penal e Direito Processual Penal pela Verbo Educacional. Bacharela em Direito (FADISMA). Rio Grande do Sul. Brasil. E-mail: duartehendrisy@gmail.com. Orcid: https://orcid.org/0000-0002-4751-7600

[2] Doutor em Direito pela Universidade Federal de Santa Catarina, na área de concentração em Relações Internacionais, com período de realização de Estágio de Doutorado com bolsa da CAPES na Università Degli Studi di Padova - Itália. Professor Associado I no Departamento de Direito da Universidade Federal de Santa Maria (UFSM), em regime de dedicação exclusiva e no Programa de Pós-Graduação em Direito da UFSM (Mestrado). Coordenador do Programa de Pós-Graduação em Direito da Universidade Federal de Santa Maria. Coordenador do CEPEDI (Centro de Estudos e Pesquisas em Direito e Internet). Rio Grande do Sul. Brasil. E-mail: rafael.oliveira@ufsm.br. Orcid: https://orcid.org/0000-0001-5060-9779

transparência ativa e passiva, é apresentada como essencial para legitimar o uso dessa tecnologia. Contudo, índices baixos de transparência demonstram a implementação opaca e sem supervisão adequada. O estudo também critica o capitalismo de vigilância, que mercantiliza dados pessoais e instrumentaliza o comportamento humano, aprofundando desigualdades sociais. Conclui-se que o Estado deve equilibrar a eficiência tecnológica com a proteção dos direitos fundamentais, garantindo que o reconhecimento facial seja usado de forma ética, transparente e respeitosa à dignidade humana, evitando a perpetuação de desigualdades.

Palavras-chave: governança; reconhecimento facial; segurança pública; pós-democracia.

ABSTRACT

The study analyzes the regulation of video surveillance technologies in Brazil, focusing on the use of facial recognition and its implications for public security and fundamental rights. The research is based on the problem: how can the Brazilian State balance the technological efficiency of facial recognition in public security with the protection of fundamental rights, given the lack of specific regulation and gaps in transparency, accountability, and governance? Using the deductive method and bibliographic approach, the investigation draws on a Foucauldian perspective to analyze the ambivalent role of the State, which simultaneously protects fundamental rights and expands its power in the name of public security. The lack of specific regulation for facial recognition exposes discriminatory practices, driven by algorithmic biases and the appropriation of data by private entities, thus challenging democratic principles. Governance, grounded in active and passive transparency, is presented as essential to legitimizing the use of this technology. However, low transparency indices reveal an opaque implementation without proper oversight. The study also critiques surveillance capitalism, which commodifies personal data and instrumentalizes human behavior, deepening social inequalities. The study concludes that the State must balance technological efficiency with the protection of fundamental rights, ensuring that facial recognition is used ethically, transparently, and in a manner that respects human dignity, thereby preventing the perpetuation of inequalities.

Key words: governance; facial recognition; public security; post-democracy.

Artigo recebido em: 27/01/2025
Artigo aprovado em: 16/10/2025
Artigo publicado em: 20/10/2025
Doi: https://doi.org/10.24302/prof.v12.5797

1 INTRODUÇÃO

Este estudo busca verificar as perspectivas para regulação das tecnologias de videomonitoramento no contexto brasileiro, considerando a dupla atribuição do Estado enquanto regulador de políticas públicas e responsável pela proteção de direitos fundamentais. Utiliza-se a perspectiva das disciplinas, em Foucault, para afastar esse estudo do campo meramente jurídico, bem como o conceito de Pós-Democracia e da suspensão do corpus jurídico em prol dos interesses neoliberais característicos dessa reformulação do Estado. Observa-se que o Estado não se rege mais pelos limites legais por si mesmo impostos, os quais assumem caráter meramente formal nos modelos de origem liberal.

No primeiro capítulo, portanto, explora-se dois dos principais papéis assumidos pelo Estado Democrático de Direito, o primeiro enquanto garantidor dos direitos fundamentais de sua população e, o segundo, enquanto formulador de políticas públicas de segurança. No segundo capítulo, serão observadas as principais iniciativas de governança empregadas no uso de reconhecimento facial aplicado na segurança pública brasileira, considerando aspectos como transparência, accountability, proteção de dados e garantia dos direitos individuais. Essa observação permitirá identificar lacunas e padrões na atuação estatal, partindo-se da delimitação das competências material e legislativa entre os entes federados e dos contornos dados em um contexto de inexistência de uma norma que defina a aplicação do reconhecimento facial.

Um dos meios utilizados para embasar a tomada de decisão dos policymakers tem sido a análise de estudos que mensuram a percepção da população acerca dos principais aspectos das políticas de segurança pública como a atuação das polícias militares, a variável de interação da polícia com os sujeitos (experiências pessoais) e os impactos dessas interações com o processo de socialização. Em um contexto de

dataficação da vida[3] em que as multiplicidades são categorizadas e transformadas em produto a ser extraído em prol de uma mercantilização dos sujeitos, tem-se o aumento das bases de dados estatísticos, viabilizados pelo contexto de democracia, que demonstram o aumento da criminalidade no Brasil em relação ao período da ditadura. Não se ignora o fato de que a possibilidade de aumento desses dados estatísticos pode ser reflexo de falta de metodologia de coleta e padronização de dados durante os anos que antecederam 1988 ou de uma subnotificação proposital, que ainda reflete uma falsa percepção de que nos anos de autoritarismo explícito no Brasil (de 1964 a 1985, mais precisamente) não havia índices de criminalidade.

Nesse contexto, percebe-se a ascensão das tecnologias de vigilância enquanto ferramenta que permite "vigiar e controlar os movimentos de forma ampla, mas que oculta em sua oposição o policiamento de um número reduzido de pessoas" (Amaral, 2018, p. 538). As justificativas para a adoção de tais sistemas perpassa argumentos como a otimização dos recursos humanos das forças de segurança (permitindo que uma pessoa operando um sistema vigie uma multidão) e a suposta neutralidade imbuída nessas tecnologias. Entretanto,

> [...] reconhecer a história das tecnologias exige considerar também que a própria noção clássica de Estado e de soberania está flexibilizada pela transnacionalização de burocracias das agências de controle que se estabelecem ao menos desde três critérios: no desenvolvimento de práticas de exceção, na elaboração de perfis e controle de estrangeiros e na normatização da mobilidade (Amaral, 2018, p. 538).

Inevitável pensar que a falta de debate sobre os vieses inerentes às tecnologias aplicadas à segurança pública leva à compreensão quase pacificada no âmbito da

[3]"O *data tsunami* que vivemos nos empurra descontroladamente seguindo um vetor imparável que digitaliza nossa existência e dificulta nosso poder de escolha. Vítimas de seu impulso, que bloqueia de forma crescente e irreversível nossa capacidade de decisão pessoal e coletiva. A supersaturação de informação está propiciando um fenômeno de delegação decisória. Renunciamos a decidir levados por uma angústia de fazê-lo. A desculpa é dupla: nos libertamos do incômodo de decidir e contribuímos para fazer mais eficientes suas consequências" (Lassale, 2019).

população geral que acredita ser desnecessário compreender os meios usados pela tecnologia, desde que atinja seus fins. Muito dessa crença se deve ao discurso de complexidade que foge à capacidade geral de entendimento, afastando também a responsabilidade de programadores e desenvolvedores em tornar acessível à sociedade o funcionamento dessas máquinas, sobretudo ao considerar que "os sistemas de Inteligência Artificial, em sua maioria, não são construídos e dirigidos exclusivamente aos setores públicos" (Giacomolli, 2023, p. 52).

O debate sobre as funções estatais na elaboração de políticas de segurança pública deve levar em consideração a transição do Estado Democrático de Direito para o surgimento de um Estado de Pós-Democrático. Sob essa ótica, o Estado se reveste da prerrogativa tecnológica a fim de distanciar os seus agentes do rótulo de perpetuadores de desigualdades e renova o discurso da política de segurança pública baseada em dados.

Nesse contexto, reitera-se a importância do debate acerca dos deveres do Estado, sobretudo ao se considerar que os tomadores de decisão constituem um grupo minoritário que, embora eleitos democraticamente, concorrem entre si e tomam a função de impor aos demais (a maioria) as decisões tomadas pelo governo (Bobbio, 2014). Funda-se, assim, a necessidade de se explorar as funções do Estado enquanto figura dicotômica na elaboração da política de segurança pública e na preservação dos direitos fundamentais da população para, então, observar as estratégias de governança no uso do reconhecimento facial na segurança pública.

2 O ESTADO AMBIVALENTE: SEGURANÇA PÚBLICA E A PRESERVAÇÃO DOS DIREITOS FUNDAMENTAIS

Ter em mente o contexto de ascensão da tecnologia enquanto ferramenta aplicada ao controle social exercido por intermédio das políticas de segurança pública permite perceber, também, o surgimento de figuras que acompanham esse

desenvolvimento da sociedade. Emerge a figura do securitizado enquanto destinatário das políticas de segurança e que serve de modelo de cidadão para os políticos tomadores de decisão. Nessa relação entre formuladores e usuários das políticas de segurança, os primeiros não se veem como pertencentes à subclasse homogeneizada pela dataficação na qual enquadram os segundos. Trabalha-se com a heterogeneidade da sociedade entre esses dois grupos enquanto possibilidade de favorecimento do centrismo político, impondo obstáculos à alternância política no poder e fomentando a polarização entre blocos políticos e enfraquecendo a democracia (Hardt; Negri, 2014; Han, 2018).

Utiliza-se, aqui, da afirmação de que o Estado é uma "realidade compósita", que sugere que ele não deve ser visto como uma entidade única e homogênea, mas sim como um conjunto complexo e dinâmico de interações entre diversos atores e instituições. Essa perspectiva, influenciada por Michel Foucault e outros teóricos, implica que o Estado é formado por múltiplos elementos que interagem de maneiras variadas, refletindo uma diversidade de interesses, práticas e relações de poder (Foucault, 2021). Quando se diz que o Estado não é uma “instituição unívoca”, significa que ele não possui uma única função ou identidade fixa. Em vez disso, o Estado é um “macroator” composto por uma pluralidade de “atores menores”, como instituições governamentais, organizações não governamentais, empresas e cidadãos, todos interligados por uma rede de relações. Essas conexões são fundamentais para entender como o Estado opera na prática, pois as ações e decisões do Estado são influenciadas por interações e pela dinâmica entre os diferentes atores envolvidos (Bruno *et al.*, 2018).

Acerca disso, merece destaque a diferenciação proposta por Zygmunt Bauman nos diálogos com David Lyon entre a aplicabilidade da figura do ban-óptico proposta por Didier Bigo e do panóptico foucaultiano. O primeiro

> [...] guarnece as entradas daquelas partes do mundo dentro das quais a vigilância do tipo 'faça você mesmo' é suficiente para manter e reproduzir a 'ordem'; basicamente, ele barra a entrada de todos os que não possuem nenhuma das ferramentas adequadas para isso [...]; e que, portanto, não podem ser considerados confiáveis no que se refere à prática dessa vigilância por conta própria (Bauman; Lyon, 2013, p. 65).

Enquanto o segundo pensa na vigilância a partir do confinamento, do "cercar do lado de dentro" (Bauman; Lyon, 2013, p. 65). Essa divisão dos indivíduos permite, ainda, uma adaptação dos tipos de vigilância empregada, se no ban-óptico é observável a premissa da exclusão, o não permitir adentrar determinados locais/recintos após a pronta identificação dos indivíduos e sua categorização enquanto dispostos ao rompimento dos padrões ali impostos; no panóptico, produz-se a disciplina através da individualização e vigilância constantes, em um processo de retroalimentação do exercício de poder sem a necessidade de ostentação de força ou coação física (Hoffman, 2018).

Administram-se os corpos de modo a afirmar completamente o potencial de vida de modo a não mais reduzir a existência humana a uma unidade produtiva (contexto de fábrica), mas para que ela integre uma massa homogeneizada produto de adestramento social, que poderá ser moldada e manuseada de acordo com os interesses de grandes instituições, sejam elas públicas ou privadas (Han, 2018). Essa "nova" forma de vigilância proporcionada pela implementação de tecnologias digitais não pode ser comparada com os modelos de panópticos originais pois esses novos modelos estão hiperconectados e operam com grandes volumes de dados em alta velocidade, funcionalizando processos de controle e vigilância nunca antes previstos (Morais, 2018). Essa adaptação dos mecanismos de vigilância que agem nas duas frentes (exclusão dos indivíduos em certos locais e vigilância furtiva). O enfraquecimento dos processos democráticos prejudica o desempenho do papel político dos tomadores de decisão que, no lugar de representarem os interesses da coletividade (real) através da autoridade exercida no governo, vão considerar uma

construção simbólica (o securitizado) enquanto destinatário da política, como representativo da coletividade (Secchi; Coelho; Pires, 2022).

Para que o Estado de Direito funcione efetivamente, é necessário um poder político forte que possa garantir e promover os direitos e deveres estabelecidos na constituição. No entanto, essa força política deve ser acompanhada de um sentimento coletivo de compromisso com os princípios constitucionais, especialmente aqueles que enfatizam a solidariedade e a dignidade humana (Morais, 2018). A falta desse compromisso tem consequências negativas. Se no capitalismo de produção, (início do século XX), a divisão do trabalho era percebida como uma forma de união entre os povos, especialmente no contexto daqueles que seguiram a onda migratória daquele período, com a transição para o capitalismo de plataformas, o comportamento humano foi moldado para que os usuários priorizassem os benefícios oferecidos pelas novas tecnologias. Assim, ficou em segundo plano o fato de que o produto dessas interações também seria capitalizado e utilizado para prever comportamentos, retroalimentando a estrutura capitalista (Zuboff, 2020).

Han disserta sobre o caminhar da sociedade para uma "era da psicopolítica digital, que avança da vigilância passiva ao controle ativo, empurrando-nos, assim, para uma nova crise da liberdade: até a vontade própria é atingida" (Han, 2018, p. 23). Observa-se aí o atual ápice do liberalismo econômico, onde a pessoa "se positiviza em coisa quantificável, mensurável e controlável" (Han, 2018, 23). Percebe-se, portanto, o enfraquecimento do poder estatal que se vê confrontado com a alta fragmentação para desempenhar suas atribuições originárias enquanto garantidor dos direitos sociais, levando a um permanente estado de reforma inspirado pelo neoliberalismo alheio às práticas produtivas.

Pensar no ciclo de políticas de segurança pública enquanto busca por soluções políticas diante do manancial de possibilidades, demanda o chamamento do gestor da administração pública (o político propriamente dito) à tomada de decisão sobre "qual caminho que ações governamentais, processos, táticas, estratégias ou programas com

potencial de consubstanciar algum tipo de política devem seguir" (Vilela, 2020, p. 54). Encontra-se nesse processo o imbricamento entre a securitização da segurança pública e a elaboração de uma política de segurança, vez que a tomada de decisão vai se embasar na identificação do destinatário e no problema público a partir de estudos elaborados pelos agentes de inteligência estratégica, que objetivam prestar auxílio na previsão de ameaças futuras.

A partir do diagnóstico apresentado, em uma tentativa de antever fatores de risco e encontrar oportunidades dentro de um cenário menos incerto, busca-se otimizar o trabalho político, porém ignora-se a quebra de isonomia entre os atores participantes (*policytakers*, tomadores de decisão etc.), o que demandaria um pensar político pautado na paridade de participação.

A problematização envolve a própria formação da individualidade dos cidadãos que, em prol de uma segurança que faz uso irrestrito da justificativa do interesse público, renunciam aos direitos à privacidade, à liberdade de expressão, informação, comunicação e opinião e à inviolabilidade da intimidade (afinal, não há garantias de que o alcance das câmeras fique restrito aos espaços públicos), da honra e da imagem.

O agir politicamente em um contexto de paridade de participação, portanto, não poderia partir de uma noção equivocada do *policytaker*, sob o risco de se contaminar todo o ciclo de políticas públicas que leva o Estado à busca pelas respostas aos seguintes questionamentos: Qual é o problema público? Problema para quem? Como o Estado define isso? Essas perguntas estariam sob o prisma de securitização do sujeito (e, portanto, da sociedade), demandando a dicotomia de que para garantir a incolumidade de determinado cidadão, tenha-se a demarcação de um inimigo a ser combatido. Evidencia-se que a tomada de decisão na implementação de políticas públicas voltadas à garantia de direitos sociais tem sua origem nos grupos minoritários que integram os círculos de poder (Arretche, 2018).

Nesse contexto, as normas operam por meio da normalização, estabelecendo critérios que antecipam comportamentos e atitudes desejadas. Isso significa que, em vez de simplesmente impor regras (normatividade), as normas buscam moldar a realidade social ao definir o que é considerado "normal" e aceitável. Por possuírem caráter político, para além da regulação dos comportamentos e por influenciarem a dinâmica social, as normas tornam-se instrumentos de controle que se sobrepõem a uma segunda natureza dos sujeitos, moldando suas ações e interações de acordo com os padrões ditados (Chignola, 2015).

Zuboff traz a ideia do poder instrumentário como essência do capitalismo de vigilância, um tipo de poder que consegue gerar o capital com base na instrumentalização do comportamento humano. "'Instrumentalização' denota as relações sociais que orientam os titeriteiros para a experiência humana como capital de vigilância a nos transformar em meios para alcançar os objetivos alheios de mercado" (Zuboff, 2020, p. 402). A instrumentalização do comportamento humano descrita por Zuboff é especialmente preocupante por subverter relações sociais e reduzir indivíduos a "meios" para fins mercadológicos, o que representa uma inversão dos valores democráticos e humanistas que deveriam nortear as sociedades contemporâneas.

Essa análise aponta para uma desumanização inerente ao capitalismo de vigilância, no qual o ser humano é reduzido a dados e mercadoria. A metáfora dos "titeriteiros" evoca uma relação de controle absoluto, em que a autonomia individual é dissolvida em prol dos interesses econômicos. Zuboff (2020) denuncia que essa lógica mercadológica não apenas explora, mas redefine as dinâmicas sociais, erodindo a privacidade e a autodeterminação. Assim, o conceito de poder instrumentário nos convoca não apenas à crítica, mas também à busca de alternativas que reumanizem as relações sociais e priorizem os direitos fundamentais frente à lógica mercantil.

Nesse contexto onde o poder das instituições apresenta um descompasso ante a ascensão de um novo poder (instrumentário), faz-se necessário (re)pensar o papel do

Estado enquanto garantidor de direitos sociais frente à expansão das fronteiras pelo ciberespaço onde o *big data* e a supervalorização das liberdades individuais enfraquece o poder emanado pelo Estado ao deixar de fora a limitação do poder exercido pelas *big techs* no contexto da sociedade de vigilância. Hodiernamente, o debate se concentra na necessidade de controle da internet ou de plataformas digitais, há uma negligência ao controle que o próprio Estado exerce sobre a população. Em nome da segurança, "sempre hipotética e nunca alcançada" (Amaral; Dias, 2024, p. 69), o Estado manipula dados pessoais para monitorar e controlar comportamentos. Sob a justificativa da segurança, as medidas de controle resultam em vigilância constante e erosão das liberdades civis.

O reconhecimento desses desafios permite problematizar também o processo de tomada de decisão nos quesitos de racionalização dos gastos públicos que levam ao investimento nos setores considerados essenciais. Sob essa bandeira, limita-se a atuação do Estado sob uma lógica atuarial, uma abordagem que utiliza métodos estatísticos e probabilísticos para avaliar e gerenciar riscos, especialmente no contexto do sistema de justiça criminal (Dieter, 2013). Essa lógica se concentra na previsão de comportamentos futuros com base em dados históricos e perfis de indivíduos, priorizando a eficiência na prevenção e controle da criminalidade em vez de investigar as causas subjacentes do crime. No contexto do sistema de justiça criminal, a lógica atuarial é aplicada para identificar e neutralizar indivíduos considerados de alto risco, como reincidentes crônicos, utilizando ferramentas de prognóstico de risco. Essa abordagem pode levar a uma "incapacitação seletiva", onde certos grupos são alvo de medidas repressivas, muitas vezes sem considerar os direitos fundamentais ou as garantias processuais, o que resulta em desigualdades e seletividade na aplicação da justiça (Dieter, 2013).

Utiliza-se dessa inter-relação para demonstrar que a lógica atuarial afasta a lei penal do seu *lócus* de aplicação, trazendo um aspecto mais gerencial de grupos de risco (distante da noção de justiça). Essa perspectiva tem início na execução penal, mas

permeia diversas etapas do procedimento criminal, mesmo na fase que antecede sua judicialização (Giacomolli, 2023). Substitui-se o componente humano e reduzem-se as experiências à cálculos matemáticos, simplificam-se complexidades de características (físicas ou de personalidade) a modelos e transforma-se os atores de um sistema de segurança em meros gestores de estatísticas e modulações, desconsiderando que modelos, por sua essência, são simplificações que não conseguem capturar toda a complexidade do mundo real ou as sutilezas da comunicação humana. Como resultado, inevitavelmente deixam de fora algumas informações relevantes.

Pensa-se a política a partir de uma ótica excludente, que define parte da sociedade como merecedora do direito à segurança, enquanto relega outra à noção de inimiga. O Estado enquanto instrumento que perpetua a seletividade do sistema penal, utiliza-se da vigilância e das novas tecnologias para justificar práticas discriminatórias que antecedem o próprio alcance do judiciário e muitas vezes inviabilizam a ingerência de qualquer outro tipo de controle sobre tais práticas. Amaral e Dias (2024) constatam que o discurso da segurança é frequentemente utilizado como uma justificativa para a manutenção de desigualdades sociais e para a repressão de determinados grupos. A imposição dessa visão do Estado à população fomenta o contexto da guerra civil que ilustra as democracias securitárias e:

> [...] não é mais suficiente e satisfatório apenas crer nas políticas de segurança promovidas pelo estado por meio do poder de polícia, pelo contrário, a segurança se trata de uma responsabilidade-compartilhada, isto é, um dever permanente das pessoas (sujeito segurança) contra qualquer ameaça ou risco à segurança (Dias; Santos; Amaral, 2023, p. 131).

Supera-se a noção de que o Estado detém o uso "legítimo" da força para exercer o controle social, principalmente porque não há mais o exercício da força bruta, tão somente. Naturaliza-se a vigilância em massa sob o deslocamento da responsabilidade pela segurança pública e enraíza-se a ideia de que para se ter segurança, também é

preciso renunciar à própria privacidade. O discurso da segurança é uma narrativa que enfatiza a necessidade de proteger a sociedade de ameaças, muitas vezes apresentando a vigilância como uma solução necessária. Esse discurso pode ser manipulado para justificar ações que, de outra forma, poderiam ser vistas como invasivas ou discriminatórias. Por exemplo, a ideia de que "precisamos monitorar mais para garantir a segurança" pode levar a políticas que aumentam a vigilância em comunidades já marginalizadas (Amaral; Dias, 2024). Esse discurso não pode ser analisado isoladamente, assim como toda política pública, é importante considerar os impactos sociais durante a implementação e essa perspectiva pode ser trazida a partir de mecanismos de oportunidade para entidades e para a sociedade civil integrarem o debate pública sobre os temas (Kremer; Nunes; Lima, 2023).

A questão é observada a partir da descentralização da responsabilidade estatal, especialmente sob a lógica da governamentalização do poder. Em vez de manter um monopólio da violência e do controle, o Estado colabora com comunidades e outras agências para “promover” a segurança e a prevenção, refletindo uma abordagem mais flexível e adaptativa, de forma negativa, ao delegar a empresas privadas a manipulação de tecnologias aplicadas à segurança pública, como o reconhecimento facial (Chignola, 2015). O deslocamento do poder de execução dessas políticas do Estado para o setor privado, pela entrega de meios de coleta e armazenamento de dados com chancela pública, também consolida assimetrias de conhecimento e controle. Problematiza-se, ainda, a presença constante de metadados, como a criação de perfis baseados em estereótipos, a aplicação de penalidades com base em probabilidades, a vigilância por meio de associações e a diminuição do direito à privacidade, pois, em que pese essas atividades não sejam exercidas por entidades públicas, o fazem em nome do Estado. Desse modo, atribui-se ao governo a responsabilidade de adotar ações para prevenir esses possíveis perigos (Dijck, 2017).

Segundo Zuboff (2020), os dados coletados pelas empresas de tecnologia transformam-se em mercadorias dentro de uma nova fase do capitalismo, que não

busca apenas prever ou controlar comportamentos de risco, mas também extrair o que ela chama de "mais-valia comportamental". Dessa forma, os dados pessoais, expropriados por corporações privadas, convertem-se em um novo mecanismo de acumulação, que Zuboff (2020) denomina "capitalismo de vigilância". As empresas e companhias de dados, ao mesmo tempo em que competem entre si, também formam parcerias, especialmente quando se trata de ganhar e preservar a confiança dos usuários. A confiança nas políticas de dados de uma empresa pode representar um diferencial competitivo. No entanto, com o aumento das colaborações nesse setor, os usuários precisam estar sempre vigilantes em relação ao compartilhamento de dados entre essas empresas (Dijck, 2017), o que majoritariamente não é compartilhado com os usuários e, no contexto de serviços públicos, em evidente desatenção aos requisitos de transparência.

A governança da vida, portanto, envolve a conexão e troca de informações entre diferentes agências e *expertises*, que podem ser mobilizadas para monitorar e modular situações de risco. Isso implica uma colaboração que transcende as especificidades educacionais, psicológicas ou sociais, criando um sistema mais abrangente de controle e gestão que se desvencilha da atuação estatal e opera pela lógica de mercado (Chignola, 2015).

O compartilhamento dessa responsabilidade demanda que o cidadão assuma novas funções, permitindo que o Estado ofereça "como única alternativa aos que não se ajustaram ao novo modo de produção seu aparato repressivo/policial e punitivo" (Dias; Santos; Amaral, 2023, p. 132).

Emerge uma nova forma de pensar na democracia, sob a ótica da securitização, que não se institui numa total adoção de um Estado autoritário, entretanto mantém-se uma democracia formal revestida de uma estrutura institucional autoritária (Augusto, 2018), ao que se define como democracia securitária. O desenvolvimento da segurança pública brasileira foi influenciado e adaptado ao surgimento de novas tecnologias, demandando uma articulação discursiva que justificasse sua adoção:

> O arquétipo bélico para segurança pública trata-se de um dispositivo, uma estruturação política por meio da qual o sistema capitalista domina o sobejo existente e fictícios dos contingentes humanos, a segurança pública ao invés de cessar com as desigualdades inerentes aos espaços urbanos, o que acaba reforçando através de uma gerência violenta sobre a população residente nas regiões periféricas (Dias; Santos; Amaral, 2023, p. 136).

O contexto de democracia securitária dá novos contornos às práticas de controle social exercidas historicamente sobre as populações marginalizadas, entretanto, e a fim de atender aos princípios que regem o Estado Democrático de Direito, revestem-se da suposta neutralidade da tecnologia. A questão ainda ganha novas nuances diante do emprego de tecnologias desenvolvidas no âmbito privado e que têm a opacidade de funcionamento como característica inerente (Pasquale, 2015). Nesse contexto, não se pode olvidar que cientistas, agências governamentais e corporações, por motivos distintos, compartilham um grande interesse nas relações mediadas por dados e no desenvolvimento de técnicas capazes de prever e influenciar o comportamento. A busca desses agentes por compreender, prever e controlar o comportamento humano coincide em certos aspectos, mas diverge em outros. As companhias de dados desejam que suas plataformas sejam vistas como objetivas e formadas por conjuntos padronizados de metadados, considerados superiores e mais precisos do que as ferramentas usadas por agências governamentais ou acadêmicas para medir aspectos como o sentimento dos consumidores, a saúde pública ou os movimentos sociais (Dijck, 2017) Entretanto, é sempre atual a ressalva de Morozov sobre os simplismos tecnológicos, pois:

> [...] embora 'mais computação' ou 'mais informação' possam ser soluções privadas lucrativas para determinados problemas, não são necessariamente as respostas mais eficazes para problemas públicos complexos e difíceis, decorrentes de causas institucionais e estruturais profundas (Morozov, 2018, p. 39).

A adoção irrestrita da tecnologia para tratamento de problemas públicos complexos (como é a criminalidade) evidencia uma tentativa do Estado em distanciar-

se do agir segregador sob a justificativa da prevenção (Castro; Pedro, 2010). Sob essas condições admite-se que o Estado adote uma postura onipresente e onisciente, colocando em jogo a articulação de controle, segurança, visibilidade, risco e liberdade e explicite a dicotomia presente.

A gestão dos fluxos de dados aparenta estar imersa nas complexidades das delimitações territoriais pouco claras. A questão do acesso e das restrições aos dados está em disputa tanto no espaço público quanto em áreas que ficam fora do conhecimento geral das pessoas (Dijck, 2017). A vigilância exercida por meio da tecnologia de videomonitoramento é indissociável de outros dispositivos, por exemplo, ainda que se tenha um sistema automatizado de coleta e captura de faces por meio da biometria, em algum momento poderá ser necessário que os agentes de segurança pública interpelem algum dos indivíduos reconhecidos por esse sistema (Castro; Pedro, 2010).

Pensar na vigilância exercida pelo Estado em um contexto neoliberal demanda observar sua instituição normativa. Se a Constituição de 1988 instituiu um novo período democrático, mesmo assim não rompeu com alguns dos paradigmas que norteavam o período ditatorial que a antecedeu, quais os papéis do Estado em relação à segurança pública que se instituiu após? A redação constitucional permite observar a chamada da população para uma responsabilidade compartilhada com o Estado quando o assunto é segurança pública. Contudo, problematiza-se a adoção desse chamado enquanto justificativa para que o Estado mitigue o debate sobre a implementação de novas tecnologias à segurança pública.

Evidencia-se a falta de rompimento com os paradigmas de outrora, manteve-se uma estrutura institucional autoritária ao mesmo tempo em que se incorporaram princípios de liberdade inerentes à democracia. Justifica-se, assim, a adoção de medidas autoritárias sob o pálio da segurança, que, por sua vez, tem como objeto o inimigo social comum (e incerto), o qual o Estado deve combater e a população vigiar (Dias; Santos; Amaral, 2023).

O contexto permite algumas inovações no conceito de segurança, se antes era tratada em equiparação à segurança externa, a segurança interna, aqui posta como a segurança pública propriamente dita, desvela uma atuação descentralizada, delimitada e multiplicada entre os diversos atores que compõem a nação (Dias; Santos; Amaral, 2023). Dessa forma, "em nome da segurança, políticas se espalham rizomaticamente, utilizam novas tecnologias e, assim, dispersam sua dinâmica" (Opitz, 2012, p. 09).

> As invocações contemporâneas da segurança não se adequam nem ao entendimento criminológico de segurança conforme a lei, tampouco à delinquência controlada. A mera violação de uma lei não circunscreve as questões levantadas pelas atuais invocações de segurança – um desenvolvimento que é, paradoxalmente, acompanhado pelo uso prolongado de categorias como 'criminoso' e 'intruso' no cenário internacional (Opitz; 2012, p. 09).

Ressalva-se essas inovações no conceito de segurança, propondo uma análise sobre a forma como são moldados o domínio e a lógica exercidos pelos atores políticos ou não. Opitz (2012, p. 10) problematiza a forma como é afastada a ponderação de se querer garantir a segurança, afirmando que "a política moderna está preocupada com a questão de *como* garantir a segurança". Sob esse prisma, a segurança afasta relações de soberania para que se tornem relações de segurança, se antes o pensar governamental demandava a renúncia de direitos individuais a fim de erradicar a desordem natural, sob a perspectiva liberal a governamentalidade vai exercer a limitação seletiva. Exerce seu poder de forma ilimitada às populações que se pretende controlar e o limita diante daquelas que não demandam o exercício da segurança, mas tão somente o seu direito abstrato (Foucault, 2023).

Indissociáveis, portanto, as relações da utilidade da população com o modelo liberal de governamentalidade, sobretudo ao se considerar a roupagem economicista atribuída à própria existência humana. Essa furtividade no exercício do poder pelo governo é instrumentada por estruturas de contingências onde as liberdades são

produzidas deliberadamente e organizadas para melhor proveito do Estado e, portanto, da economia. Não se exerce tão somente o poder pela coerção direta e pela violência explícita, mas articulam-se os discursos para promoção de uma atuação repressiva em consonância com os princípios democráticos. As disciplinas possuem um discurso próprio que não se confunde com o do direito, sendo este discurso distinto da lei e da regra enquanto manifestação da vontade soberana (Foucault, 2021). O discurso das disciplinas está relacionado à norma, estabelecendo um código que não é o da lei, mas o da normalização. Elas [as disciplinas] se baseiam em um horizonte teórico que não pertence ao campo jurídico, mas sim ao âmbito das ciências humanas.

Os limites impostos pelo Estado não se dão exclusivamente vinculados à disposição jurídica, eles são observados pela perspectiva da economia política e constituem o que Foucault definiu por governamentalidade[4].

A aplicação das tecnologias de segurança, nesse contexto, visa delimitar até onde o poder governamental atua de forma insidiosa e passa a tornar obrigatórias as medidas a fim de assegurar uma liberdade estritamente produtiva (Opitz, 2012). Reside aí o ponto nevrálgico da problematização do presente estudo, uma vez que a ascensão do neoliberalismo na sociedade brasileira encontra não só as tecnologias de segurança de outrora, mas também aquelas elaboradas no contexto de um capitalismo de vigilância, que vem sendo aplicado nas relações privadas e extrapola esse limite ao ser replicado pelo ente público. Ao analisarem essas adaptações, Augusto e Wilke dissertam que:

> A biopolítica não é extinta, porém, não é a-histórica, e tende a ser ultrapassada por outras tecnologias de poder contemporâneas. Foucault passa a interessar-se cada vez mais pela governamentalidade e pelas crises da governamentalidade. É também no mesmo ano em que o Nascimento da biopolítica é proferido no Collège de France (1979), que Theodore Schultz é

[4]"[...] uma certa naturalidade própria da prática de governo e a autolimitação da razão governamental baseada numa racionalidade de governo liberal: a demarcação entre agenda e não agenda, conforme Jeremy Bentham. A validade das práticas de governo não será mais medida em termos de legitimidade, mas de seu sucesso" (Augusto; Wilke, 2019, p. 225).

> laureado com o Prêmio Nobel de Economia pela teoria do capital humano, uma radicalização das teorias neoliberais gestadas no pós-nazismo e no pós-Guerra (Augusto; Wilke, 2019, p. 226).

É sobre essa adaptação das tecnologias contemporâneas que se observa a dicotomia que o presente estudo se debruça: um Estado que é ao mesmo tempo garantidor da segurança e da proteção de direitos fundamentais. Afinal, a construção do Estado neoliberal embasa-se no paradigma de segurança que, se fosse possível expressar de forma matemática, conteria como variáveis a pobreza, a moral, a economicidade e a governamentalidade dos corpos (Opitz, 2012; Foucault, 2023). Nesse contexto, vê-se uma mudança da biopolítica tradicional, que se apropria de dados demográficos para controle de modo estatístico, para uma apropriação de dados psicográficos (por meio do perfilamento de dados e preferências). A partir do contexto neoliberal, o *big data* permite a extração de um perfilamento coletivo de populações e grupos (Han, 2018).

O enquadramento da pobreza e da luta de raças enquanto inimigas morais da sociedade tem sido o pano de fundo do desenvolvimento das políticas de segurança pública. Ao se aplicar a lógica economicista fomentada pelo neoliberalismo, "o indivíduo perigoso paga o preço por não ser capaz de ser governado por meio da simultânea produção e consumo da liberdade" (Opitz, 2012, p. 14), ele contrasta com os indivíduos governáveis e demanda o tratamento disciplinar (Foucault, 2010).

Ao "se permitir" ser governado, o indivíduo se coloca em uma classe vista pela não-intervenção do Estado e ao mesmo tempo, paradoxalmente, justifica a própria intervenção do estado a fim de garantir os processos que se veem permanentemente ameaçados pelo indivíduo perigoso. Sven Opitz declara que esse o ponto crucial do paradoxo, "não é um erro ou uma falha a ser dissipada para o bem do suave funcionamento governamental. Muito pelo contrário: é o mecanismo-chave da governamentalidade liberal" (Opitz, 2012, p. 14).

As dinâmicas sociais, ainda que de forma ilusória, constroem-se a partir dessa relação entre inclusão e exclusão de tipos de perigo de maior ou menor grau (Castro; Pedro, 2010). Se para ter segurança é necessário renunciar à privacidade (e, consequentemente, aos demais direitos decorrentes disso), relativiza-se o seu custo a partir do afastamento do debate sobre os problemas envolvidos, ao mesmo passo em que se aumenta a percepção de insegurança de viver-se em espaços que não estão sujeitos à vigilância do Estado.

3 RECONHECIMENTO FACIAL E A LACUNA REGULATÓRIA: ESTRATÉGIAS DE LEGITIMAÇÃO NA SEGURANÇA PÚBLICA A PARTIR DA GOVERNANÇA

A observação dos instrumentos de organização social é inerente ao estudo do Direito, uma vez que são sua razão de ser nas sociedades politicamente organizadas. Entretanto, para além de uma perspectiva positivista, a adaptação da sociedade ao incremento do reconhecimento facial na segurança pública demanda um olhar às noções universais que instrumentalizam o Direito. A prática jurídica é composta por elementos de conexão que permitem o uso diretivo da linguagem para influir no comportamento da sociedade por meio de condutas prescritas (Coelho, 2008). Para compreender as nuances envolvidas nessa instrumentalização por intermédio de normas, lança-se mão das palavras de Foucault ao dispor que:

> [...] no caso da teoria do governo não se trata de impor uma lei aos homens, mas de dispor as coisas, isto é, utilizar mais táticas do que leis, ou utilizar ao máximo as leis como táticas. [...] Isso assinala uma ruptura importante: enquanto a finalidade da soberania é ela mesma, e seus instrumentos têm a forma de lei, a finalidade do governo está nas coisas que ele dirige, deve ser procurada na perfeição, na intensificação dos processos que ele dirige e os instrumentos do governo, em vez de serem constituídos por leis, são táticas diversas (Foucault, 2021, p. 418).

O surgimento do processamento computadorizado de dados mudou os paradigmas sobre a proteção dos indivíduos contra o poder informacional das empresas de tecnologias e do Estado, uma vez que um amplo espectro de dados pessoais, até então considerado juridicamente irrelevante, passou a ter relevância (Gleizer; Montenegro; Viana, 2021). Essa transformação, no entanto, não inaugurou a proteção jurídica da personalidade humana e dos dados pessoais. Já havia dados pessoais juridicamente relevantes, como os protegidos pelos direitos de sigilo, a exemplo das informações trocadas por cartas ou por telefone. O diferencial trazido pelo processamento computadorizado de dados está no fato de que, mesmo dados considerados menos significativos, ou seja, aqueles que, à primeira vista, não revelariam informações pertinentes à vida privada, podem, quando combinados e comparados a outros, fornecer informações sensíveis ou até mesmo possibilitar a criação de perfis de personalidade dos indivíduos (Gleizer; Montenegro; Viana, 2021).

Pensar essas estratégias tem sido um dos muitos desafios enfrentados pelos burocratas brasileiros ao tentar estruturar os objetivos constitucionais propostos pela Constituição de 1988. Seriam esses os limites às ingerências estatais que justificam a inviolabilidade dos direitos "à vida, à liberdade, à igualdade, à segurança e à propriedade" (Brasil, 1988). Entretanto, problematiza-se o equívoco interpretativo ao equiparar a inviolabilidade à intangibilidade; a primeira, define-se pela vedação à intervenção injustificada, ao passo que a segunda remete à ideia de intocável (Gleizer; Montenegro; Viana, 2021).

Ainda, é necessário entender outra distinção dogmática: a que se faz entre direitos submetidos à reserva de lei simples, à reserva de lei qualificada e direitos sem reserva de lei. Algumas normas do Art. 5º da CF, que trata dos direitos fundamentais, incluem cláusulas de reserva de lei simples, nas quais o legislador pode autorizar intervenções. Outras normas possuem reserva qualificada, permitindo intervenções apenas para determinadas finalidades ou em circunstâncias específicas, exigindo o cumprimento de certos pressupostos para que a intervenção seja legítima. Por fim, há

normas que parecem oferecer uma proteção absoluta em comparação com as anteriores, pois, ao afirmar o direito, o constituinte silencia quanto à imposição de reservas. A esse terceiro grupo, dos direitos fundamentais sem reserva de lei, pertence, por exemplo, o direito à livre manifestação do pensamento (Gleizer; Montenegro; Viana, 2021).

O constituinte não estabeleceu condições que permitiriam intervenções nesses direitos, mas também não os definiu como absolutos. A única manifestação indireta a favor de uma proteção absoluta encontra-se no Art. 60, §4º, da CF, que trata do conteúdo essencial dos direitos fundamentais (Gleizer; Montenegro; Viana, 2021). Assim, uma interpretação mais coerente e vantajosa seria considerar esses direitos como sujeitos a uma proteção ampliada, o que implicaria maior rigor na justificação de eventuais intervenções. Mesmo aceitando que direitos fundamentais sem reserva possam ser objeto de restrições, eles estariam, em geral, subordinados a duas exigências: primeiro, que essas restrições estejam legalmente fundamentadas, não se diferenciando, nesse aspecto, dos direitos sujeitos à reserva de lei; e, segundo, que tais direitos só possam ser limitados quando houver a necessidade de proteger outros valores de hierarquia constitucional (Gleizer; Montenegro; Viana, 2021).

Essas questões ganham relevância ao pensar que a lacuna legislativa sobre segurança pública vem sendo preenchida por alguns preceitos previstos no Código de Processo Penal e que os limites da intervenção do Estado no âmbito dos direitos fundamentais têm ganhado novos contornos em uma sociedade cada dia mais automatizada. Desse modo, observar os mecanismos e estratégias de implementação da tecnologia de Reconhecimento Facial na segurança pública a partir de requisitos estipulados pelo próprio Estado é essencial para compreender porque uma das premissas é a impossibilidade de um uso democrático do RF no contexto atual. Além disso, debruçar-se sobre a governança como diretriz de implementação do RF permite compreender de que forma a implementação dessa tecnologia vem sendo justificada

como ferramenta legítima de controle e vigilância social massificada, conforme demonstrado por Bu:

> A lei normalmente fica atrás da tecnologia, e o AFR atualmente existe em um vácuo regulatório, portanto, no momento está sendo usado de maneiras que minam a confiança pública nos sistemas dos quais se utilizam. Entidades privadas podem começar a usá-lo sem declarar publicamente o movimento ou notificar as autoridades. Como tal, dado a falta de um regime que regule o uso de AFR e as capacidades de rastreamento biométrico, é necessário que seja apresentada uma legislação que busque governar as tecnologias biométricas atuais e futuras. Um código de prática estatutário é necessário para reger como a polícia deve usar essa tecnologia (Bu, 2021, p. 122).

A constatação trazida por Bu (2021) ilustra como a velocidade do direito não tem sido suficiente a acompanhar o desenvolvimento da tecnologia como um todo, sobretudo ao considerar que o desenvolvimento dessas ferramentas ocorre quase que exclusivamente por empresas privadas e que estão alheias ao debate público sobre as problemáticas envolvidas na implementação irrestrita de tecnologias de vigilância e controle social. Em conclusão, Bu propõe um "código de práticas" para governança sobre o uso do RF pela polícia (Bu, 2021).

Inviável distanciar este estudo das justificativas apresentadas pelo poder público, que residem majoritariamente em questões de otimização da atividade policial, manutenção do rastreamento de criminosos e contraventores em potencial (Bu, 2021). Entretanto, reitera-se que as justificativas apresentam vieses de eficiência pautados por uma ótica de competitividade fomentada pelo contexto neoliberal e embasada em práticas autoritárias.

Busca-se compreender quais são as principais iniciativas do Estado no emprego do reconhecimento facial aplicado à segurança pública brasileira. Assim, a pesquisa se estreita à observação das estratégias adotadas pelo Estado ao formular e coordenar o uso do reconhecimento facial como ferramenta de segurança pública, partindo-se da premissa de inexistência de uma norma regulatória específica.

A partir dos parâmetros utilizados pelo governo federal, conceitua-se a governança pública como:

> [...] a aplicação de práticas de liderança, de estratégia e de controle, que permitem aos mandatários de uma organização pública e às partes nela interessadas avaliar sua situação e demandas, direcionar a sua atuação e monitorar o seu funcionamento, de modo a aumentar as chances de entrega de bons resultados aos cidadãos, em termos de serviços e de políticas públicas. (Brasil, 2020, p. 15).

Bu (2021) disserta sobre a importância de uma estrutura robusta de governança a fim de se evitarem abusos de direitos fundamentais. Utilizar-se de parâmetros de governança permite incluir a participação de múltiplos agentes interessados (governos, empresas, organizações da sociedade civil e a população), para garantir que diferentes perspectivas e preocupações sejam consideradas. Ao olhar a partir da governança, observa-se a necessidade de estabelecerem-se normas e diretrizes claras sobre o uso do RF, sobretudo pois ela também pode incluir mecanismos de supervisão e auditoria para monitorar a implementação da tecnologia e garantir que ela não seja utilizada de forma discriminatória ou abusiva (Bu, 2021).

Sem se ignorar o desafio de implementação do Reconhecimento Facial mesmo em democracias consolidadas, utiliza-se os parâmetros de transparência, *accountability*, a ótica da proteção de dados e a garantia dos direitos individuais. Com isso, busca-se identificar qual a base normativa da tomada de decisão para implementação dessa tecnologia, sob a observação das lacunas e padrões de atuação estatal. Se o Estado Democrático de Direito se embasa em parâmetros de governança e, portanto, deve envidar esforços no sentido de promover boas práticas no desenvolvimento de suas atividades, sua guinada para o viés neoliberal de gestão da segurança pública demanda um olhar crítico da academia às estratégias que legitimam o uso do reconhecimento facial. A questão ganha mais relevância ao considerar que a própria governança vem de um contexto empresarialista para ser aplicado pelo poder público,

o que reforça a lógica mercadológica inerente à perspectiva neoliberal. Acerca disso, Bevir disserta que:

> Os cidadãos, sendo atores racionais, tentam maximizar seus interesses de curto prazo, privilegiando as políticas de bem-estar que os beneficiam como indivíduos, em vez dos efeitos de longo prazo, cumulativos e compartilhados resultantes do aumento dos gastos estatais. De maneira semelhante, os políticos, sendo atores racionais, tentam maximizar seus interesses eleitorais de curto prazo, promovendo políticas que obterão os votos dos cidadãos racionais, em vez de perseguir a responsabilidade fiscal (Bevir, 2011, p. 106).

Delimita-se, portanto, as competências material e legislativa do Estado, com vistas a compreender de que forma um governo pautado em princípios de governança implementa o reconhecimento facial sem considerar as implicações éticas e legais. Na gênese de qualquer debate público devem ser consideradas as consequências da inserção de tecnologia, especialmente em uma democracia cuja atuação da administração pública está ao pálio do princípio de eficiência estatal. As implicações éticas e políticas disso, sobretudo sob a influência do neoliberalismo, levam à desvalorização da democracia e, consequentemente, dos direitos fundamentais (Marcellino Júnior, 2007). A adoção irrestrita da eficiência direciona a administração pública à lógica de mercado que valoriza a competitividade em detrimento de preceitos éticos como a dignidade humana e a justiça social. Desse modo, o emprego do direito é voltado para justificar a busca por eficiência, frequentemente de forma cínica, contribuindo para a manutenção da exclusão e marginalização de grupos sociais. A eficiência, portanto, não deve ser vista como um fim em si mesma e deve ser indissociável de outros princípios que promovam os direitos humanos e a democracia (Marcellino Júnior, 2007).

Observa-se uma postura gerencialista do Estado na implementação da tecnologia de reconhecimento facial como ferramenta de segurança pública. Ao utilizar os parâmetros de governança como filtros pelos quais o problema desta pesquisa será analisado, é necessário abordar os mecanismos de transparência

inerentes à implementação da tomada de decisão pública. A transparência é entendida como a abertura e clareza na comunicação de informações e processos governamentais ao público (Lima, 2024). Isso inclui não apenas a disponibilização de dados, mas também a forma como esses dados são apresentados. Também é considerada um elemento essencial para a responsabilização dos órgãos públicos e como mecanismo de controle, mediante fiscalização e avaliação de políticas públicas e por mecanismos de prestação de contas.

A transparência subdivide-se em dois principais eixos: ativa e passiva. A primeira, refere-se à divulgação proativa de informações pelos órgãos públicos e significa que as instituições governamentais devem disponibilizar informações relevantes sobre o uso de tecnologias de reconhecimento facial sem que os cidadãos precisem solicitar. Exemplos de transparência ativa incluem a publicação de relatórios, dados sobre a eficácia das câmeras e do sistema, informações sobre os custos envolvidos e detalhes sobre como os dados coletados são tratados. A transparência ativa é crucial porque permite à sociedade o acesso imediato e contínuo às informações, promovendo um ambiente de confiança e responsabilidade (Lima, 2024). A segunda forma de transparência (passiva) ocorre quando as informações são disponibilizadas apenas mediante solicitação, geralmente através da Lei de Acesso à Informação (LAI) (Lima, 2024). Isso significa que os cidadãos precisam fazer pedidos formais para obter dados sobre o uso de reconhecimento facial, o que pode ser um processo mais demorado e burocrático. A transparência passiva é importante, mas pode ser insuficiente se as informações não forem facilmente acessíveis ou se os órgãos públicos não responderem de maneira adequada e em tempo hábil.

A combinação de ambas as formas de transparência é essencial para garantir que a sociedade esteja informada sobre como as tecnologias de reconhecimento facial estão sendo utilizadas. Isso não apenas permite que os cidadãos compreendam melhor as implicações dessas tecnologias em suas vidas, mas também promove um debate mais amplo sobre a eficácia e a ética do uso do reconhecimento facial na segurança

pública (Lima, 2024). A falta de transparência leva a abusos, desconfiança e a uma percepção negativa sobre a utilização dessas tecnologias, enquanto uma abordagem transparente pode ajudar a construir confiança entre o governo e a população, assegurando que os direitos dos cidadãos sejam respeitados.

A ausência de mecanismos de responsabilização e prestação de contas, somada aos obstáculos que dificultam o acesso às informações sobre a implementação, impede não apenas a população, mas também os pesquisadores — vinculados a organizações públicas ou privadas — de exigir explicações acerca do funcionamento e da necessidade de adoção dessas tecnologias (Bu, 2021). A falta de transparência nas informações sobre os projetos de reconhecimento facial implica que muitos detalhes cruciais permanecem desconhecidos pelo público, como quem gerencia os dados, de que forma esses dados são armazenados e quais são os critérios para a utilização das câmeras (Bu, 2021; Lima, 2024). Essa opacidade impede os cidadãos de acessar informações essenciais que poderiam ajudá-los a compreender o impacto dessas tecnologias em suas vidas, reforçando a possibilidade de abusos de poder devido à incapacidade de questionar as ações do governo. Sem essas informações, os cidadãos não conseguem entender plenamente como o uso de tecnologias de vigilância afeta suas vidas, o que gera sentimentos de impotência e desconfiança em relação às instituições governamentais. Além disso, essa falta de transparência dificulta a participação ativa da sociedade em debates sobre políticas públicas relacionadas à segurança e à privacidade.

Uma pesquisa conjunta entre o CESec e o Lapin resultou no desenvolvimento de um índice de transparência, criado para medir a disponibilidade e a qualidade das informações relacionadas aos projetos de reconhecimento facial ranqueados pela iniciativa O Panóptico. Esse índice possibilita uma análise mais crítica e informada sobre a forma como essas tecnologias estão sendo implementadas. Como resultado, verificou-se que:

> Mais de 70% deles têm um índice de transparência inferior a quatro, sendo que aproximadamente 18% apresentam índice igual a zero. Apenas o projeto municipal de São Paulo obteve a nota máxima (sete pontos) em termos de transparência ativa devido à quantidade e à qualidade das informações fornecidas. Ressalta-se que, mesmo assim, ainda não há informações claras sobre o uso operacional de TRF. Em contraste, 34% dos projetos não pontuaram em transparência ativa, o que significa que em 17 iniciativas não há qualquer informação disponível. Boa parte da amostra concentrou-se entre três e cinco pontos. A soma desses projetos equivale a 56% do total. [...] Dos 50 projetos analisados, 22 não obtiveram nenhuma pontuação. Ou seja, em 44% da amostra não obtivemos um retorno considerável e/ou não recebemos resposta alguma ao pedido de informação (Lima, 2024, p. 33).

O índice considera aspectos como a disponibilidade de informações, se os dados sobre os projetos estão acessíveis ao público incluindo detalhes sobre como as tecnologias estão sendo utilizadas; qualidade das informações, ao avaliar se as informações disponíveis são claras, completas e úteis para compreensão do impacto do uso do RF (Lima, 2024). Destaca-se que o estudo verificou que muitos projetos de RF carecem de dados sobre fornecedores, custos e relatórios de impacto. A falta dessas informações essenciais impede que a sociedade faça uma avaliação crítica e embasada sobre a implementação do RF. Sem dados claros, é difícil para os cidadãos, pesquisadores e formuladores de políticas entenderem os riscos, benefícios e implicações éticas envolvidas (Bu, 2021; Lima, 2024).

Mecanismos de transparência têm o condão de permitir a responsabilização de órgãos públicos diante da violação de direitos fundamentais da população. Quando as informações não estão disponíveis ou são difíceis de acessar, a capacidade da sociedade de monitorar e avaliar a atuação do governo é comprometida, o que viola princípios do Estado Democrático de Direito, sobretudo num contexto de securitização. A transparência também é crucial para construir e manter a confiança do público nas instituições. Quando as operações são auditáveis e os dados sobre o uso da tecnologia são acessíveis, isso permite que haja um controle mais rigoroso sobre possíveis abusos ou violações de direitos (Bu, 2021). A supervisão e auditoria ajudam a identificar e corrigir práticas inadequadas, promovendo um uso mais responsável

da tecnologia. Se os cidadãos sentem que não têm acesso às informações necessárias, isso pode minar a confiança nas políticas públicas e nas tecnologias implementadas.

Com um sistema de supervisão e auditoria em funcionamento, é possível identificar rapidamente quaisquer abusos ou violações de direitos que possam ocorrer. Por exemplo, se houver evidências de discriminação no uso do RF ou de vigilância excessiva, esses mecanismos podem ajudar a detectar essas práticas inadequadas (Bu, 2021). Uma vez identificados, os problemas podem ser corrigidos, seja por meio de ajustes nas políticas, treinamento adicional para os operadores da tecnologia ou até mesmo a suspensão do uso do RF em determinadas circunstâncias.

Além disso, a supervisão e auditoria promovem um uso mais responsável da tecnologia, pois criam um ambiente em que as entidades que utilizam o RF são incentivadas a agir de maneira ética e a considerar as implicações de suas ações. A possibilidade de revisão e responsabilização pode levar as organizações a serem mais cautelosas e a implementar melhores práticas, viabilizando que a tecnologia seja utilizada de forma a respeitar os direitos individuais e a dignidade das pessoas (Bu, 2021). Entretanto, no contexto analisado neste estudo, observa-se que a opacidade das tecnologias atualmente empregadas, aliada à falta de regulamentação, impede a criação de um cenário adequado para a implementação de mecanismos que possibilitem a supervisão e a readequação do uso do RF na segurança pública.

As questões envolvendo a necessidade de transparência estão intrinsecamente ligadas à *accountability*, sobretudo por se tratar, em um sentido mais amplo, da responsabilidade pública de forma geral. Sendo a segunda [*accountability*] mais abrangente, congrega aspectos como a ética, a própria transparência e a necessidade de prestação de contas, surgindo como um princípio de governança essencial para problematizar o uso indiscriminado do RF na segurança pública (Bu, 2021; Duong, 2018). A falta de diretrizes para uso do RF também denota a ausência de estrutura de responsabilidade, pois as entidades que fazem uso podem agir de maneira arbitrária, aplicando o RF como modo de vigilância excessiva e discriminatória.

Inerente ao excesso de vigilância, tem-se o processamento (coleta, armazenamento e tratamento) de dados pessoais em larga escala e sem finalidade inicial explícita. Ao implementar o reconhecimento facial na segurança pública, tem-se uma "diluição da responsabilidade que se verifica na atribuição à tecnologia de agência sobre decisões relacionadas na abordagem, identificação, tipificação ou condenação" (Silva, 2022, p. 113). Entretanto, considerando a necessidade de vinculação das decisões dos agentes públicos, verifica-se que a ampla margem de discricionariedade concedida aos gestores no uso dessas tecnologias pode resultar em decisões arbitrárias e na ausência de mecanismos que garantam a proteção dos direitos dos titulares de dados (Reis *et al.*, 2021). Essa situação cria um ambiente em que a responsabilidade pública é comprometida, devido à falta de diretrizes claras que orientem o uso dessas ferramentas.

Verifica-se, ainda, que não existem informações sistemáticas e publicamente disponíveis que detalhem como as tecnologias de vigilância estão sendo empregadas, quais dados estão sendo coletados e quais resultados estão sendo alcançados. Sem esses dados, é difícil para o público, pesquisadores e órgãos de controle avaliarem a eficácia e a legalidade das ações do governo (Reis *et al.*, 2021). Sem dados claros e acessíveis, torna-se inviável responsabilizar os gestores públicos por suas decisões e ações. Se não há informações sobre como as tecnologias estão sendo utilizadas, é difícil identificar possíveis abusos ou falhas na implementação, o que leva à impunidade.

Soma-se a isso a dependência e submissão das instituições públicas a tecnologias e serviços fornecidos por grandes corporações internacionais. Silveira denomina essa dependência de "epistemicídio", conceito que se refere à destruição ou marginalização de saberes e conhecimentos de grupos subalternos. Esse fenômeno não se limita a questões raciais, mas abrange um regime de verdade que sustenta a colonialidade (Cassino; Souza; Silveira, 2021). Essa colonialidade é reforçada por práticas que se tornaram normais e acríticas, sustentadas por estruturas que promovem a alienação técnica. Essas estruturas são fundamentais para o

funcionamento do neoliberalismo em uma sociedade intensamente *dataficada*, na qual os dados são coletados e utilizados de forma a beneficiar grandes corporações. Diante desse cenário, surge a necessidade de uma postura mais colaborativa e de incentivo à criatividade local.

Ainda no interior da *accountability*, é importante observar as implicações éticas do uso do RF na segurança pública. O reconhecimento facial tem demonstrado uma tendência a falhar na identificação precisa de indivíduos de diferentes etnias, especialmente aqueles com pele mais escura (Duong, 2018). Isso se deve, em parte, à falta de diversidade nos conjuntos de dados utilizados para treinar os algoritmos de reconhecimento facial. Quando esses sistemas são desenvolvidos com dados predominantemente de indivíduos de pele clara, eles tendem a ser menos eficazes em reconhecer e identificar corretamente pessoas de outras etnias, resultando em taxas mais altas de falsos positivos e negativos.

O banco de dados utilizado para análise das imagens capturadas em tempo real é desenvolvido no contexto de criação da ferramenta de reconhecimento facial. Pariser (2012) argumenta que, ao utilizar tecnologias baseadas em algoritmos de predição, a ferramenta de aprendizado de máquina aprende conforme os bancos de dados com os quais é alimentada. Ou seja, se os bancos de dados utilizados contêm predominantemente informações de indivíduos negros ou pardos, a tendência de o algoritmo considerar essa característica como um fator determinante aumenta significativamente (Kremer; Nunes; Lima, 2023). Se os dados utilizados para treinar esses algoritmos refletem preconceitos históricos ou práticas discriminatórias, o resultado pode ser uma vigilância desproporcional sobre comunidades marginalizadas. Isso significa que, em vez de melhorar a segurança, a tecnologia pode aumentar a criminalização e a opressão dessas populações.

Se a polícia tem um histórico de direcionar suas operações para certas comunidades com base em racismo, misoginia, homofobia, aprofobia e outros tipos de preconceitos, os dados coletados refletirão essa prática. Quando esses dados são

usados para treinar algoritmos, o resultado pode ser uma previsão de criminalidade que continua a direcionar a polícia para essas mesmas comunidades, perpetuando um ciclo de vigilância, violência e criminalização. Isso não apenas prejudica a confiança da comunidade nas forças de segurança, mas também pode levar a um aumento da tensão social e da marginalização (Kremer; Nunes; Lima, 2023). A vigilância excessiva pode resultar em estigmatização, discriminação e violação de direitos civis. Além disso, a falta de representação e voz nas decisões sobre como essas tecnologias são implementadas pode levar a um sentimento de impotência e desconfiança em relação às instituições.

A aplicação desigual da tecnologia, onde algumas áreas têm restrições rigorosas, enquanto outras podem operar com pouca ou nenhuma supervisão gera inconsistências que podem criar um ambiente onde as normas de privacidade não são respeitadas de maneira uniforme, atingindo diretamente o princípio constitucional da isonomia (Bu, 2021). O reconhecimento facial permite que indivíduos sejam identificados e monitorados em tempo real, muitas vezes sem o seu conhecimento ou consentimento. Isso levanta sérias questões éticas sobre a capacidade de vigilância das autoridades e empresas, criando um ambiente onde impera a violação da privacidade (Bu, 2021). Uma vez que os dados biométricos são coletados e armazenados, eles podem ser difíceis de apagar completamente. Essa "persistência de dados" significa que informações pessoais podem ser mantidas indefinidamente, aumentando o risco de uso indevido ou vazamentos (Duong, 2018; Zuboff, 2020). A preocupação aqui é que, mesmo que um indivíduo não deseje mais ser monitorado, seus dados podem continuar a ser acessíveis e utilizados, nem sempre para os objetivos inicialmente propostos (como para fins de “promoção” da segurança pública) (Pasquale, 2015). Com isso, oculta-se o fato de que muitos dos que tentam proteger seus dados ou apagar seus rastros digitais (sombra digital) acabam atraindo a atenção do sistema de controle justamente por realizar essas ações.

Soma-se à problemática os vieses raciais, de gênero e de classe inerentes ao contexto de criação dessas tecnologias (Buolamwini; Gebru, 2018; Kremer; Nunes; Lima, 2023). Todo o contexto de desenvolvimento da sociedade brasileira é moldado a partir de suas raízes discriminatórias, assim, a análise de vieses algorítmicos é crucial para entender como a tecnologia falha não apenas em reconhecer indivíduos de maneira adequada, mas também ao perpetuar estereótipos e injustiças (Bu, 2021). A ideia de uma "vigilância perpétua" refere-se à capacidade de monitorar indivíduos continuamente, o que pode levar à erosão de direitos fundamentais, como a liberdade de expressão e o direito à privacidade.

A vigilância constante pode criar um ambiente de medo e autocensura, no qual as pessoas se sentem menos livres para se expressar ou agir de maneira autêntica, temendo que suas ações sejam observadas e julgadas. A inibição das individualidades gera problemas como a perda de diversidade e criatividade, a pressão pelo conformismo, o aumento de tensões e divisões sociais, a desvalorização da autenticidade e da autoestima, além da dificuldade na resolução de conflitos. Esses fatores limitam o potencial de inovação e a capacidade de diálogo entre diferentes grupos, gerando desconfiança e enfraquecendo a coesão social. Como resultado, tanto o bem-estar individual quanto o coletivo são comprometidos.

O desenvolvimento da tecnologia influencia a sociedade ao desfigurar as individualidades de coletividades, especialmente em um contexto em que não há debate público sobre as problemáticas relacionadas ao uso do reconhecimento facial (RF). Isso é agravado pela falta de literacia digital, que impede o uso consciente de ferramentas cotidianas, como celulares e computadores. A questão deve ser analisada também à luz das práticas de neocolonialismo, especialmente porque essas práticas se manifestam na imposição de formas de pensar, agir e se comportar que desqualificam ou ignoram os saberes e métodos de aprendizado de comunidades e sociedades menos favorecidas, em um contexto cada vez mais mercantilizado (Cassino; Souza; Silveira, 2021). Além disso, essa nova colonialidade exclui a autonomia, a busca por alternativas

e qualquer esforço de resistência aos interesses da economia e das grandes corporações do conceito de normalidade. Retomando o conceito de enxame (Han, 2018; Berardi, 2019), tem-se uma sociedade dominada pelos simplismos tecnológicos e,

> Nessa conjuntura, a relação entre os elementos participantes - corpos, dados, fluxos e máquinas - acaba sendo regulada por um princípio de conexão automática, em que as ações e condutas de cada integrante deve respeitar automatismos interiorizados, pois apesar de corpos conscientes, estes são passivos e não essenciais (Giacomolli, 2023, p. 50).

Quando o RF é utilizado de forma abrangente, a expectativa de não ser monitorado ou registrado sem consentimento é comprometida, pois diante da situação de constante vigilância, ocorre a inibição de comportamentos naturais e espontâneos. Para além dos aspectos da privacidade, instaura-se um ambiente de medo e autocensura e, em uma era do "cancelamento", seja na internet ou no mundo real, a distorção dos contextos e falas também é uma constante de medo na população (Bu, 2021). Quando uma pessoa sabe que está sob vigilância, pode temer as consequências de suas ações ou expressões, incluindo o receio de represálias por opiniões ou afiliações políticas, comportamentos considerados inadequados ou até por interações sociais comuns (Amaral; Salles; Medina, 2020). Esse temor pode inibir tanto a liberdade de expressão quanto a participação ativa na vida pública.

Não se ignora o fato de que os direitos à privacidade e à proteção contra interferências arbitrárias não são absolutos; eles são considerados "qualificados" (Bu, 2021; Giacomolli, 2023). Em certas circunstâncias, pode haver justificativas legais para restringir tais direitos, desde que essas restrições sejam necessárias e proporcionais. No entanto, essa qualificação também abre espaço para abusos, pois pode ser difícil determinar quando uma restrição é realmente justificada e quando se torna arbitrária ou ilegal. Isso inclui a vigilância em massa, a coleta de dados sem consentimento e a utilização da tecnologia para fins discriminatórios ou punitivos. A falta de supervisão

pode resultar em situações em que a tecnologia é empregada para monitorar e controlar populações, exacerbando problemas de discriminação e injustiça social (Bu, 2021).

A problemática ganha novas cores ao pensar na expressão "caixa-preta" cunhada por Pasquale e atribuída para definir a sociedade atual, pois serve como uma metáfora devido ao seu duplo significado. Ele pode designar um dispositivo de gravação, como os sistemas de monitoramento de dados utilizados em aviões, trens e carros (Pasquale, 2015, p. 3). Alternativamente, pode se referir a um sistema cujo funcionamento permanece misterioso; embora seja possível observar suas entradas e saídas, não se consegue compreender como uma se transforma na outra. Vê-se nesse tipo de funcionamento uma violação a todos os princípios de governança utilizados como parâmetros para esta pesquisa.

Ao abordar algumas leis e jurisprudências sobre o uso do reconhecimento facial ao redor do mundo, Bu (2021) observa que, embora uma proibição total possa parecer uma solução, ela negaria os benefícios e a conveniência que o reconhecimento facial (RF) pode oferecer, caso seja bem desenvolvido. Embora a perspectiva apresentada por Qingxiu Bu possa sugerir um olhar excessivamente positivo — o qual esta autora não endossa —, ele destaca que as legislações sobre privacidade seriam a "pedra angular" para a adoção de medidas que viabilizem um uso mais adequado do RF. Isso porque tais legislações permitiriam a adoção de medidas fundamentadas em avaliações de impacto, possibilitando uma adequação das instituições que utilizam essa tecnologia.

Dada a importância que a privacidade assume nos estudos sobre reconhecimento facial aplicado à segurança pública, destaca-se não se ignorar o Projeto de Lei (PL) 1.515/2022, que até o momento da redação final desta pesquisa ainda está em trâmite. Entretanto, reitera-se que o foco desta pesquisa estava voltado para a análise da governança em um contexto em que ainda subsiste a lacuna legislativa, o que certamente não esgota o tema central. Desse modo, compreende-se que esta pesquisa agrega o cenário de problematização envolvendo alguns dos vários aspectos

do emprego de tecnologias de vigilância pelo Estado e que o escopo de uma dissertação não permite abordar com a profundidade necessária todos os aspectos envolvidos.

4 CONSIDERAÇÕES FINAIS

Explorou-se a fundamentação teórica que embasa a implementação do reconhecimento facial na segurança pública, abordando suas implicações legais e sociais. Nesse contexto, constata-se a necessidade de uma estrutura normativa que regule o uso do reconhecimento facial, levando em consideração os direitos fundamentais e a proteção da privacidade dos cidadãos como princípios norteadores dessa norma. Essa regulamentação não pode estar dissociada de princípios éticos e democráticos, nem fazer uso de mecanismos ocultos. A análise se apoia nos conceitos de governança e *accountability*, ressaltando a importância da transparência nas ações do Estado, bem como a imposição de requisitos alinhados a esses conceitos ao contratar empresas para fornecer a tecnologia.

Além disso, explorou-se a relação entre a segurança pública e a construção social do medo, destacando como a percepção de insegurança pode influenciar a aceitação de tecnologias invasivas, como o reconhecimento facial. Quando a população se sente ameaçada pela criminalidade, tende a apoiar medidas que prometem aumentar a segurança, mesmo que tais medidas envolvam invasões de privacidade. A crítica de Foucault sobre o controle social é utilizada para sugerir que o reconhecimento facial tem sido empregado como uma ferramenta de vigilância, perpetuando desigualdades e discriminações. A discussão enfatiza a necessidade de um equilíbrio entre segurança e direitos individuais, propondo que a regulamentação do uso dessas tecnologias seja orientada por princípios éticos e democráticos, sem que estes fiquem em segundo plano em relação à eficiência, como ocorre no contexto atual.

Recorreu-se às críticas de Michel Foucault sobre controle social para argumentar que tecnologias de vigilância estão sendo utilizadas para monitorar e controlar a população, perpetuando desigualdades sociais e discriminações. O reconhecimento facial, nesse contexto, é visto como uma ferramenta que não apenas identifica indivíduos, mas também reforça estigmas e marginaliza grupos já vulneráveis.

Verificou-se que mecanismos de transparência e prestação de contas são essenciais para a participação pública, sobretudo se estiverem alinhados a uma postura emancipatória da população e pelo estímulo aos saberes locais. Entretanto, somente esses mecanismos não são suficientes para salvaguarda de direitos fundamentais, sobretudo ao considerar que eles sequer são aplicados no contexto atual de implementação do RF como ferramenta de segurança pública. Logo, tampouco ratificam a implementação do RF na segurança pública, porque não se considera uma necessidade de prestação de contas à sociedade sobre os motivos pelos quais essa tecnologia é aplicada.

Por fim, no que diz respeito à discrepância entre o uso da governança como suporte para a implementação do reconhecimento facial (RF) e a obrigação de salvaguarda dos direitos fundamentais, observa-se que a securitização da sociedade tem corrompido até mesmo a noção de inviolabilidade desses direitos. Ao analisar o distanciamento do Estado de princípios democráticos sob o argumento de que o direito à segurança prevalece sobre as liberdades individuais, constata-se uma acentuação de cisões históricas, sejam elas raciais ou sociais. Assim, o Estado tem priorizado a eficiência em detrimento da promoção dos direitos humanos e da própria democracia, agindo com base na lógica atuarial de gestão de riscos matematicamente construídos. Esse descompasso compromete a confiança da população tanto no Estado, enquanto garantidor de direitos fundamentais, quanto na relação de confiança entre os próprios cidadãos.

Ao fim e ao cabo, verifica-se que a lacuna normativa sobre o uso do reconhecimento facial (e de tecnologias de vigilância em geral) continua sendo preenchida pela aplicação irrestrita de medidas previstas no Código de Processo Penal, quando ficam restritas à regulação por portarias sem ter força obrigacional perante particulares. No entanto, essa legislação é incapaz de abordar adequadamente questões sociais historicamente perpetuadas na sociedade brasileira. Essa situação abre espaço para a adoção reiterada de medidas autoritárias por parte do Estado na gestão de políticas de segurança, o que se torna ainda mais evidente em um contexto de digitalização das interações sociais.

Portanto, é evidente a necessidade de uma mudança cultural que promova a emancipação tecnológica da população, permitindo que ela se desvincule de pressupostos ideológicos enraizados na sociedade e continuamente reforçados pela dataficação. Torna-se essencial estimular a criticidade e até formas de insurgência que questionem a implementação do reconhecimento facial (RF), que ainda ocorre de maneira discreta e pouco transparente.

REFERÊNCIAS

AMARAL, A. J. Biopolítica e biocapitalismo: implicações da violência do controle. **Veritas**, Porto Alegre, v. 63, n. 02, p. 515-543, maio/ago. 2018. Disponível em: https://doi.org/10.15448/1984-6746.2018.2.30794. Acesso em: 12 mai. 2023.

AMARAL, A. J.; DIAS, F. V. **Tecnopolítica Criminal**. 1. ed. São Paulo: Tirant lo Blanch, 2024.

AMARAL, A. J.; SALLES, E. B. C.; MEDINA, R. S. Urbanização Militarizada e Controle Social: primeiras impressões sobre os "drones" como dispositivos de segurança pública no Brasil. **Revista de Direito da Cidade**, v. 11, n. 2, p. 278-298, 2020. Disponível em: https://www.e-publicacoes.uerj.br/rdc/article/view/35835. Acesso em: 12 out. 2023.

ARRETCHE, M. Democracia e redução da desigualdade econômica no Brasil. **Revista Brasileira de Ciências Sociais**, v. 33, n. 96, p. 1-23, 2018. Disponível em: https://www.scielo.br/j/rbcsoc/a/Mtx4F43dy9YjLkf9k85Gg7F/abstract/?lang=pt . Acesso em: 19 ago. 2022.

AUGUSTO, A. Trinta anos esta noite: busca por segurança e medidas autoritárias na Constituição federal de 1988. **Revista História**: Debates e Tendências, v. 18, n. 3, p. 380 - 391, 2018. Disponível em: https://seer.upf.br/index.php/rhdt/article/view/8595. Acesso em: 25 ago. 2023.

AUGUSTO, A.; WILKE, H. Racionalidade neoliberal e segurança: embates entre democracia securitária e anarquia. *In*: RAGO, M.; PELEGRINI, M. (Orgs.). **Neoliberalismo, feminismos e contracondutas?** Perspectivas foucaultianas. São Paulo: Intermeios, 2019, v. 1, p. 225-245.

BERARDI, F. **Depois do futuro**. [recurso eletrônico]. São Paulo: Ubu Editora, 2019.

BEVIR, M. Governança democrática: uma genealogia. **Rev. Sociol. Polit.**, v. 19, n. 39, p. 103-114, jun. 2011. Disponível em: https://www.scielo.br/j/rsocp/a/YkZsZbDQpz94zmpNdrRWwyt/?format=pdf&lang=pt . Acesso em: 11 out. 2024.

BOBBIO, N. **Qual democracia?** São Paulo: Edições Loyola, 2014.

BOULAMWINI, J.; GEBRU, T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 81, p. 1-15, 2018. Disponível em: https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Acesso em: 01 out. 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 mar. 2023.

BRASIL. Tribunal de Contas da União. **Referencial básico de governança aplicável a organizações públicas e outros entes jurisdicionados ao TCU/Tribunal de Contas da União**. 3. ed. Brasília, TCU, Secretaria de Controle Externo da Administração do Estado – SecexAdministração, 2020. Disponível em: https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-e-programas/integra/gestao-do-conhecimento/publicacoes/referenciais-externos/referencial_basico_governanca_orgaos_entidades.pdf/view. Acesso em: 10 out. 2024.

BRUNO, F. *et al.* (Orgs.). **Tecnopolíticas da vigilância:** perspectivas da margem. 1. ed. São Paulo: Boitempo, 2018. E-book.

CASARA, R. R. R. **Estado pós-democrático:** neo-obscurantismo e gestão dos indesejáveis. 3. ed. Rio de Janeiro: Civilização Brasileira, 2018. E-book.

CASTRO, R. B.; PEDRO, R. M. L. R. Redes de vigilância: experiência da segurança e da visibilidade articuladas às câmeras de monitoramento urbano. *In*: BRUNO, F.; KANASHIRO, M.; FIRMINO, R. (Orgs.). **Vigilância e visibilidade**: Estado, tecnologia e identificação. Porto Alegre: Sulina, 2010.

CHIGNOLA, S. A toupeira e a serpente. **Revista de Direitos e Garantias Fundamentais**, v. 19, n. 3, p. 239–269, 2018. Doi: 10.18759/rdgf.v19i3.1599.

COELHO, S. C. N. Norma Jurídica e Lei são Figuras Teóricas Diferentes. **Revista Brasileira de Estudos Políticos**, v. 98, p. 175-204, 1 jul. 2008. Disponível em: https://pos.direito.ufmg.br/rbep/index.php/rbep/article/view/73. Acesso em: 29 set. 2023

DIAS, F. V.; SANTOS, L. S.; AMARAL, A. J. Democracia securitária: implicações das políticas de segurança pacificadoras e humanizadoras. **Revista jurídica Cesumar**, v. 23, n. 1, p. 129-144, jan./abr. 2023. Disponível em: https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/11262. Acesso em: 01 jul. 2023.

DIETER, M. S. Lógica atuarial e incapacitação seletiva: a farsa da eficiente gestão diferencial das novas classes perigosas. **Revista Epos**, Rio de Janeiro, v. 4, n. 1, 2013. Disponível em: https://pepsic.bvsalud.org/scielo.php?pid=S2178-700X2013000100003&script=sci_abstract. Acesso em: 01 jul. 2024.

DIJCK, J. Confiamos nos dados? As implicações da datificação para o monitoramento social. **MATRIZes**, São Paulo, Brasil, v. 11, n. 1, p. 39–59, 2017. Disponível em: https://revistas.usp.br/matrizes/article/view/131620. Acesso em: 23 out. 2024.

DUONG, J. *et. al*. **A Technological and Ethical Analysis of Facial Recognition in the Modern Era**. UCLA, 2018. Disponível em: https://www.academia.edu/38066258/A_Technological_and_Ethical_Analysis_of_Facial_Recognition_in_the_Modern_Era. Acesso em: 08 jun. 2023.

FOUCAULT, M. **Em defesa da sociedade**; tradução Maria Ermantina Galvão. 2. ed. São Paulo: WMF Martins Fontes, 2010.

FOUCAULT, M. **Microfísica do poder**. 11. ed. São Paulo: Paz e Terra, 2021.

FOUCAULT, M. **Segurança, território, população:** curso dado no Collége de France (1977-1978); tradução de Eduardo Brandão; revisão de tradução de Cláudia Berliner. 2. ed. São Paulo: Martins Fontes, 2023.

GIACOMOLLI, F. **Gerenciamento tecnológico do sistema de justiça penal**: as novas tecnologias no âmbito do policiamento, da investigação e da decisão. Rio de Janeiro: Marcial Pons, 2023.

GLEIZER, O.; MONTENEGRO, L.; VIANA, E. **O direito de proteção de dados no processo penal e na segurança pública**. Rio de Janeiro: Marcial Pons, 2021.

HAN, B.-C. **Psicopolítica:** o neoliberalismo e as novas técnicas de poder. Tradução Maurício Liesen. Belo Horizonte: Editora Âyiné, 2018.

HARDT, M.; NEGRI, A. **Declaração:** isto não é um manifesto. Tradução: Carlos Szlak. São Paulo: N-1 edições, 2014.

HOFFMAN, M. O poder disciplinar. *In*: TAYLOR, D (Ed.). **Michel Foucault:** conceitos fundamentais. Petrópolis: Vozes, 2019. p. 41-57.

KREMER, B.; NUNES, P.; LIMA, T. **Racismo algorítmico**. Rio de Janeiro: CESeC, 2023. E-book.

LASSALLE, J. M. **Ciberleviatán**: El colapso de la democracia liberal frente a la revolución digital. [recurso eletrônico]. Barcelona: Arpa Editores, 2019.

LIMA, T. **Vigilância por lentes opacas:** mapeamento da transparência e responsabilização nos projetos de reconhecimento facial no Brasil. Rio de Janeiro: CESeC, 2024. Disponível em: https://drive.google.com/file/d/1i7bBfb86pO6-y9WgnKiL_04yez8dP9cG/view . Acesso em 20 out. 2024.

MARCELLINO JUNIOR, J. C. O princípio constitucional da eficiência administrativa e a ética da libertação: uma leitura a partir da obra de Enrique Dussel. **Revista Eletrônica Direito e Política**, Itajaí, v.2, n.2, 2º quadrimestre de 2007. Disponível em: https://periodicos.univali.br/index.php/rdp/article/download/7590/4345/20372. Acesso em: 10 out. 2024.

MORAIS, J. L. B. O estado de direito "confrontado" pela "revolução da internet"!. **Revista Eletrônica do Curso de Direito da UFSM**, v. 13, n. 3, p. 876–903, 2018. Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/33021. Acesso em: 23 out. 2024.

MOROZOV, E. **Big Tech:** a ascensão dos dados e a morte da política. Tradução: Cláudio Marcondes. São Paulo: Ubu, 2018.

OPITZ, S. Governo não ilimitado – o dispositivo de segurança da governamentalidade não-liberal. **Ecopolítica**, São Paulo, n. 2, p. 03-36, 2012.

Disponível em: https://revistas.pucsp.br/index.php/ecopolitica/article/view/9075/6683. Acesso em: 15 jul. 2023.

PARISER, E. **O filtro invisível**: O que a internet está escondendo de você. Rio de Janeiro: Zahar, 2012. E-book.

PASQUALE, F. **The Black Box Society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

REIS, C. *et al.* **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, 2021. Disponível em: https://lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil/. Acesso em: 01 out. 2024.

SECCHI, L.; COELHO, F. S.; PIRES, V. **Políticas Públicas**: Conceitos, casos práticos, questões de concursos. 3. ed. São Paulo: Cengage Learning, 2022.

SILVA, T. **Racismo Algorítmico**: inteligência artificial e discriminação nas redes digitais. São Paulo: SESC, 2022.

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