UNIVERSIDADE CATÓLICA DE PERNAMBUCO
PRÓ-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO
COORDENAÇÃO DA PÓS-GRADUAÇÃO-*STRICTO SENSU*
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

VIGILÂNCIA ALGORÍTMICA E BOM POLICIAMENTO: LEGITIMIDADE DEMOCRÁTICA DO VIDEOMONITORAMENTO COM LEITURA AUTOMÁTICA DE PLACAS EM PERNAMBUCO

Marcela Melo de Freitas

Recife
2026

Marcela Melo de Freitas

VIGILÂNCIA ALGORÍTMICA E BOM POLICIAMENTO: LEGITIMIDADE DEMOCRÁTICA DO VIDEOMONITORAMENTO COM LEITURA AUTOMÁTICA DE PLACAS EM PERNAMBUCO

Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Direito da Universidade Católica de Pernambuco - UNICAP, como parte dos requisitos para obtenção do título de Mestre em Direito, Área de Concentração: Direito, Processo e Cidadania; Linha de Pesquisa: Cidadania Digital.
Orientador: Prof. Dr. Stéfano Gonçalves Régis Toscano.

Recife
2026

F866v Freitas, Marcela Melo de.
Vigilância algorítmica e bom policiamento : legitimidade democrática do videomonitoramento com leitura automática de placas em Pernambuco / Marcela Melo de Freitas, 2026.
128 f.

Orientador: Stéfano Gonçalves Régis Toscano.
Dissertação (Mestrado) - Universidade Católica de Pernambuco. Programa de Pós-graduação em Direito. Mestrado em Direito, 2026.

1. Direito - Filosofia. 2. Videovigilância. 3. Inteligência artificial. 4. Segurança pública. 5. Legitimidade (Direito). 6. Estado. 7. Democracia. 8. Direito constitucional.

CDU 340.12

Luciana Vidal - CRB-4/1338

TERMO DE APROVAÇÃO

MARCELA MELO DE FREITAS

VIGILÂNCIA ALGORÍTMICA E BOM POLICIAMENTO: LEGITIMIDADE DEMOCRÁTICA DO VIDEOMONITORAMENTO COM LEITURA AUTOMÁTICA DE PLACAS EM PERNAMBUCO

Dissertação apresentada ao Programa de Pós-Graduação em Direito, área de concentração Direito, Processo e Cidadania da Universidade Católica de Pernambuco (UNICAP) para obtenção do título de Mestre em Direito. A presente dissertação foi defendida e aprovada em 29 de abril de 2026 pela banca examinadora constituída pelos professores doutores:

gov.br Documento assinado digitalmente
STEFANO GONCALVES REGIS TOSCANO
Data: 05/06/2026 18:09:40-0300
Verifique em https://validar.iti.gov.br

Orientador(a) e Presidente da Banca: Prof. Dr. Stéfano Gonçalves Régis Toscano

gov.br Documento assinado digitalmente
VANESSA ALEXSANDRA DE MELO PEDROSO
Data: 16/06/2026 09:23:57-0300
Verifique em https://validar.iti.gov.br

Titular Interno(a) – Prof.ª Dr.ª Vanessa Alexsandra De Melo Pedroso

Alexandre Henrique Tavares Saldanha
Assinado de forma digital por Alexandre Henrique Tavares Saldanha
Dados: 2026.06.09 16:48:11 -03'00'

Titular Interno(a) – Prof. Dr. Alexandre Henrique Tavares S[illegible]

gov.br Documento assinado digitalmente
JOSE ROBERTO WANDERLEY DE CASTRO
Data: 10/06/2026 11:06:21-0300
Verifique em https://validar.iti.gov.br

Titular Externo(a) – Prof. Dr. José Roberto Wanderley De Castro

Recife

2026

“Todas as vitórias ocultam uma abdicação” (Simone de Beauvoir).

AGRADECIMENTOS

Primeiramente, a Deus, por ser a fonte de toda força e sabedoria, guiando meus passos e me sustentando em cada desafio superado ao longo desta jornada.

À minha mãe, com todo o meu amor e gratidão. Você sempre foi meu porto seguro e o molde de sustentação da minha vida. Sem o seu apoio incondicional e o exemplo de resiliência que você me deu, este sonho jamais seria possível.

Ao meu orientador, Stefano Toscano, pela dedicação e paciência. Mais do que uma orientação técnica, suas intervenções foram uma verdadeira aula de como construir uma dissertação com rigor e excelência. Sou imensamente grata por ter tido a oportunidade de aprender com sua experiência.

Ao meu namorado, pelo companheirismo constante e por ser meu maior incentivador. Obrigada por acreditar no meu potencial, por me apoiar nos dias difíceis e por me impulsionar a crescer profissionalmente. Sua presença tornou este percurso mais leve.

À minha cadela Lina, que, com sua alegria genuína e companhia silenciosa, soube transformar momentos de pressão e sobrecarga em instantes de leveza e conforto.

A todos que, direta ou indiretamente, contribuíram para a realização deste trabalho, o meu muito obrigada.

RESUMO

FRETAS, Marcela Melo. **Vigilância algorítmica e bom policiamento:** legitimidade democrática do videomonitoramento com leitura automática de placas em Pernambuco. Recife: Dissertação de Mestrado do Programa de Pós-Graduação em Direito da Universidade Católica de Pernambuco – UNICAP, 2026.

A dissertação analisa a legitimidade democrática do videomonitoramento com leitura automática de placas de veículos (LPR/ANPR) em Pernambuco, tomando como referência a ideia de bom policiamento. Parte-se do reconhecimento de que a expansão da inteligência artificial na segurança pública vem transformando a vigilância urbana ao converter a circulação em dado consultável, passível de indexação, correlação e acionamento policial. A pesquisa, de natureza jurídica e teórica, desenvolve-se por meio de revisão bibliográfica e análise documental de fontes públicas relativas à implantação do sistema no Estado. O estudo reconstrói a trajetória do videomonitoramento e da inteligência artificial, discute teorias da vigilância contemporânea, examina a centralidade da proteção de dados e as tensões ligadas às exceções voltadas à segurança pública, além de descrever a infraestrutura sociotécnica do LPR em Pernambuco. Ao final, o estudo propõe parâmetros para um modelo de legitimidade democrática da vigilância, organizados em três eixos: legitimidade territorial, responsabilidade institucional e eficácia social. Conclui-se que a compatibilidade do LPR com a democracia não pode ser aferida apenas por promessas de eficiência ou por métricas internas de atividade, mas depende do enquadramento jurídico da infraestrutura, de sua distribuição territorial, da existência de mecanismos de rastreabilidade e controle externo e da demonstração de resultados socialmente relevantes. A adoção do sistema, portanto, exige reflexão crítica sobre seletividade territorial, transparência, contestabilidade e limites normativos ao uso da vigilância algorítmica pelo Estado.

Palavras-chave: vigilância algorítmica; videomonitoramento inteligente; leitura automática de placas (LPR/ANPR); bom policiamento; legitimidade democrática.

ABSTRACT

FRETAS, Marcela Melo**. Algorithmic surveillance and good policing**: democratic legitimacy of video surveillance with automatic number plate recognition in Pernambuco. Recife: Master's Dissertation from the Postgraduate Program in Law at the Catholic University of Pernambuco – UNICAP, 2026.

This dissertation analyzes the democratic legitimacy of video surveillance with automatic number plate recognition (LPR/ANPR) in Pernambuco, using the notion of good policing as its normative reference. It starts from the recognition that the expansion of artificial intelligence in public security has been transforming urban surveillance by turning mobility into searchable data, subject to indexing, correlation, and police activation. This is a legal and theoretical study developed through bibliographical review and documentary analysis of public sources related to the implementation of the system in the state. The study reconstructs the trajectory of video surveillance and artificial intelligence, discusses theories of contemporary surveillance, examines the centrality of data protection and the tensions surrounding exceptions related to public security, and describes the socio-technical infrastructure of LPR in Pernambuco. In its final part, the study proposes parameters for a model of democratic legitimacy of surveillance, structured around three axes: territorial legitimacy, institutional responsibility, and social effectiveness. It is concluded that the compatibility of LPR with democracy cannot be assessed solely through promises of efficiency or internal activity metrics, but depends on the legal framing of the infrastructure, its territorial distribution, the existence of traceability and external oversight mechanisms, and the demonstration of socially relevant outcomes. The adoption of the system therefore requires critical reflection on territorial selectivity, transparency, contestability, and normative limits on the State’s use of algorithmic surveillance.

Keywords: algorithmic surveillance; smart video surveillance; automatic number plate recognition (LPR/ANPR); good policing; democratic legitimacy.

LISTA DE SIGLAS

AIACT	*Artificial Intelligence Act*
ANPD	Autoridade Nacional de Proteção de Dados
ANPR	*Automatic Number Plate Recognition*
CFTV	Circuito Fechado de Televisão
CIODS	Centro Integrado de Operações de Defesa Social
CNMP	Conselho Nacional do Ministério Público
CNPD	Comissão Nacional de Proteção de Dados
EBIA	Estratégia Brasileira de Inteligência Artificial
GOFAI	*Good Old-Fashioned Artificial Intelligence*
GDPR	*General Data Protection Regulation*
IA	Inteligência Artificial
LGPD	Lei Geral de Proteção de Dados Pessoais
LPR	*License Plate Recognition*
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OCR	*Optical Character Recog*nition/Reconhecimento Óptico de Caracteres
PCI	Ponto de Captura de Imagem
SDS	Secretaria de Defesa Social
UNESCO	Organização das Nações Unidas para a Educação, a Ciência e a Cultura
VMS	*Video Management System*

SUMÁRIO

1 INTRODUÇÃO 12
2 ESTRUTURA E DISCIPLINAMENTO DA VIGILÂNCIA DIGITAL 17
2.1 PERCURSO DA IMPLEMENTAÇÃO DO VIDEOMONITORAMENTO E DA INTELIGÊNCIA ARTIFICIAL 17
2.2 Lei Geral de Proteção de Dados (LGPD) E PROJETOS DE REGULAMENTAÇÃO NO BRASIL 25
2.3 EXPERIÊNCIAS INTERNACIONAIS: *AI ACT* E OUTROS MODELOS COMPARADOS 31
3 TEORIAS DO PANOPTISMO E DA VIGILÂNCIA CONTEMPORÂNEA 38
3.1 BENTHAM E FOUCAULT: PANOPTISMO, DISCIPLINA E VISIBILIDADE 38
3.2 DO PANOPTISMO À SOCIEDADE DE CONTROLE: DELEUZE E O PODER EM REDE 44
3.3 VIGILÂNCIA DIGITAL, CAPITALISMO DE DADOS E SUBJETIVAÇÃO CONTEMPORÂNEA 49
3.4 CÁRCERE, DISTÂNCIA SOCIAL E PRODUÇÃO DE VERDADE: PONTE PARA A VIGILÂNCIA ALGORÍTMICA 55
4 VIDEOMONITORAMENTO INTELIGENTE EM PERNAMBUCO COM IDENTIFICAÇÃO DE PLACAS DE VEÍCULOS 58
4.1 ESTRUTURA E EXPANSÃO DO SISTEMA DE CÂMERAS EM PERNAMBUCO 58
4.2 UTILIZAÇÃO DOS MECANISMOS DE VIGILÂNCIA PELA POLÍCIA 61
4.3 LPR E GOVERNAMENTALIDADE ALGORÍTMICA DA CIRCULAÇÃO 65
5 FORMAS DE POLICIAMENTO E A CONSTRUÇÃO DO BOM POLICIAMENTO 69
5.1 POLICIAMENTO ENTRE CONTROLE POLÍTICO E VIGILÂNCIA AUTOMATIZADA 76
5.1.1 "Síndrome dos meios sobre os fins": LPR entre a métrica de atividade e o bom policiamento em Pernambuco 81
5.2 RASTREABILIDADE E CONTROLE EXTERNO DO LPR. 88
5.3 PARÂMETROS PARA UM MODELO DE LEGITIMIDADE DEMOCRÁTICA NA VIGILÂNCIA 95
5.3.1 Legitimidade territorial: da “fobópole” à geografia da suspeição 96

5.3.2 Legitimidade como responsabilidade: controle do genoespaço pelo nomoespaço 100
5.3.3 Eficácia social como critério de legitimidade democrática 104
6 CONSIDERAÇÕES FINAIS 108
REFERÊNCIAS 114

1 INTRODUÇÃO

A expansão recente da inteligência artificial no campo da segurança pública vem alterando de modo significativo a forma como o poder estatal observa, classifica e intervém sobre a circulação no espaço urbano. No lugar de uma vigilância predominantemente humana, localizada e reativa, consolidam-se infraestruturas capazes de registrar, indexar, cruzar e acionar informações em tempo quase contínuo. Nesse cenário, o videomonitoramento deixa de ser apenas mecanismo de captação de imagens e passa a operar como tecnologia de tratamento de dados, especialmente quando associado a sistemas de leitura automática de placas de veículos (*License Plate Recognition* – LPR/ANPR).

Em Pernambuco, a implantação dessa tecnologia insere o debate sobre segurança pública em um problema que já não pode ser compreendido apenas em chave operacional ou administrativa, exigindo análise jurídica sobre limites, controles, justificações e compatibilidade com a democracia.

É precisamente nesse ponto que se situa o tema desta dissertação. O objeto da pesquisa não será a inteligência artificial em abstrato, nem a vigilância em sentido genérico, mas, a legitimidade democrática do videomonitoramento com leitura automática de placas em Pernambuco, considerada a partir da ideia de 'bom policiamento'. A investigação partirá da constatação de que a ampliação dessas tecnologias vem ocorrendo mais rapidamente do que a consolidação de critérios públicos de justificação, de mecanismos de controle e de parâmetros jurídicos suficientemente claros para enquadrar o seu uso. A questão central, portanto, não será apenas se o LPR incrementa a capacidade policial, mas, em que medida esse incremento poderá ser considerado compatível com exigências democráticas de legitimidade, limitação do poder e responsabilização.

Sob essa perspectiva, tratar-se-á de uma pesquisa jurídica, porque seu núcleo estará voltado à análise dos limites normativos e conceituais do uso estatal de tecnologias de vigilância em espaços públicos. A investigação não se limitará a descrever o funcionamento técnico do sistema. Seu objetivo será compreender como esse funcionamento se articula com exigências de uma compatibilidade democrática, especialmente em um contexto em que o tratamento de dados para fins de segurança pública permanece marcado por lacunas regulatórias, zonas de exceção e dificuldades de controle.

A relevância do tema decorre justamente dessa combinação entre expansão tecnológica e insuficiência de balizas públicas robustas. O uso do LPR não se resume a uma inovação neutra voltada ao aumento da eficiência. Ele reconfigura a relação entre vigilância, mobilidade e espaço público, ao converter o movimento cotidiano em rastro pesquisável, passível de recuperação retrospectiva, correlação com listas de interesse e acionamento policial. Isso fará com que a discussão sobre câmeras e inteligência artificial não possa ser reduzida à promessa de modernização da segurança. Ao contrário, imporá perguntas sobre quem se tornará mais visível ao Estado, sob quais critérios certos fluxos passarão a ser priorizados, quais instâncias poderão revisar o uso da ferramenta e como se preservará a dimensão pública do policiamento quando a decisão passar a depender de plataformas, parâmetros e infraestruturas técnicas cada vez mais complexas.

O problema de pesquisa poderá, assim, ser formulado de modo direto: em que medida o uso do videomonitoramento inteligente com leitura automática de placas, no contexto pernambucano, é compatível com critérios democráticos de legitimidade e com a ideia de ‘bom policiamento’? Essa formulação já pressupõe que a tecnologia não deverá ser julgada apenas por sua utilidade aparente ou por sua capacidade de produzir números de atividade. O ponto decisivo será saber se seu uso estará juridicamente enquadrado e publicamente justificado de forma suficiente para que não se converta em mera expansão de poder estatal sem equivalente expansão de garantias.

O objetivo geral desta dissertação é analisar a legitimidade democrática do videomonitoramento com LPR em Pernambuco, articulando o debate teórico sobre vigilância contemporânea, o marco jurídico relacionado à proteção de dados e à regulação da inteligência artificial e os critérios normativos de avaliação do policiamento. Para alcançar esse objetivo, a pesquisa busca, de modo específico, reconstruir a evolução do videomonitoramento e da inteligência artificial; discutir teorias do panoptismo, da sociedade de controle e da vigilância digital; examinar a centralidade jurídica da proteção de dados e as tensões produzidas pelas exceções relativas à segurança pública; descrever a estrutura do sistema pernambucano e a cadeia que liga imagem, dado, alerta e decisão; e, por fim, aplicar ao caso critérios de legitimidade extraídos da literatura sobre bom policiamento, policiamento democrático, responsabilização e controle público.

A justificativa da pesquisa está vinculada a uma dupla necessidade. Em primeiro lugar, há uma necessidade teórica de compreender de que modo o uso de inteligência artificial no policiamento altera categorias tradicionais do debate sobre vigilância, visibilidade, suspeição e poder. Em segundo lugar, há uma necessidade jurídica e institucional: discutir se a adoção de tecnologias altamente intrusivas pode ocorrer sem balizas públicas suficientemente densas sobre finalidade, rastreabilidade, controle externo e contestabilidade. O tema se mostra relevante porque toca diretamente a relação entre segurança pública e cidadania em sociedades digitalizadas, nas quais a capacidade estatal de observar e inferir cresce de forma acelerada, enquanto os mecanismos de limitação jurídica nem sempre acompanham esse movimento com a mesma velocidade.

As questões que orientam o desenvolvimento do texto são, portanto, menos tecnicistas do que pode parecer à primeira vista. Não se trata apenas de saber como funciona o LPR, mas de investigar o que ele faz juridicamente com o espaço público e com a atividade policial. Que tipo de vigilância se consolida quando a circulação urbana passa a ser transformada em dado consultável? Como a cadeia sociotécnica que liga captura, leitura, cruzamento e alerta interfere no exercício do poder policial? Quais salvaguardas são necessárias para que a tecnologia não produza apenas maior capacidade operacional, mas também atuação estatal controlável, inteligível e justificável? E, sobretudo, como a ideia de bom policiamento pode funcionar como critério para avaliar se esse uso permanecerá compatível com um horizonte democrático?

Esta investigação caracteriza-se como um estudo jurídico[1] de cunho teórico e exploratório, fundamentado em revisão bibliográfica e no exame de fontes públicas atinentes ao cenário pernambucano. O trabalho abdica de mensurações empíricas ou da reconstituição detalhada do funcionamento interno do sistema via dados sigilosos. O propósito central é realizar análise crítica dos pilares que sustentam a implementação do LPR no Estado, utilizando o acervo disponível para compreender como a tecnologia é apresentada pelo Direito, organizada nas instâncias institucionais

[1] Declaro, para os devidos fins, que utilizei a ferramenta de Inteligência Artificial Generativa ChatGPT, da *OpenAI*, na elaboração desta dissertação, especificamente para revisão gramatical e ortográfica do texto, revisão de referências bibliográficas e aprimoramento da clareza e organização textual. Ressalto que todo o conteúdo gerado por essas ferramentas foi submetido a rigorosa revisão crítica, validação de fontes e adaptação autoral. Assumo integral responsabilidade pela originalidade, veracidade e integridade de todo o conteúdo apresentado neste documento, em estrita conformidade com a Portaria CNPq nº 2.664/2026 e as diretrizes de integridade acadêmica desta instituição.

e balizada pelas normas vigentes. Por conseguinte, o eixo metodológico reside menos na observação da prática policial e mais na interpretação de marcos teóricos, legislações e registros oficiais.

Essa delimitação metodológica é importante porque permite alinhar, desde o início, o escopo da introdução ao que efetivamente será desenvolvido nos capítulos seguintes. Não se pretende realizar uma auditoria técnica do sistema, nem avaliação estatística conclusiva sobre seu desempenho concreto. O que se busca é uma análise jurídica e conceitual do problema, voltada a identificar os limites normativos, os riscos democráticos e os critérios de legitimidade que deveriam orientar o uso do videomonitoramento com LPR em Pernambuco. A reconstrução da infraestrutura pública descrita em editais, termos de referência, relatórios e materiais oficiais permite indagar se o problema jurídico do LPR se esgota em sua existência como ferramenta tecnológica ou se se estende à forma como sua arquitetura técnica é normativamente enquadrada e operacionalmente incorporada às rotinas de vigilância e decisão policial.

A estrutura da exposição parte de uma teórica geral ao caso concreto e, em seguida, ao retorno normativo e avaliativo. Os capítulos iniciais constroem o pano de fundo para compreender a vigilância algorítmica como fenômeno sociotécnico e político. Em seguida, é feita uma análise voltada ao caso pernambucano, descrevendo a expansão do videomonitoramento, a utilização dos mecanismos de vigilância pela polícia e o papel específico do LPR na governamentalidade algorítmica da circulação. Por fim, o capítulo 5 reúne os elementos normativos centrais do estudo, discutindo o que seja bom policiamento e quais critérios permitem avaliar a compatibilidade democrática do sistema. Esse capítulo também incorpora, de forma mais específica, a discussão sobre a diluição da responsabilidade na vigilância algorítmica, enfatizando a rastreabilidade e o controle externo do LPR, e culmina na proposição de parâmetros para um modelo de legitimidade democrática da vigilância, organizado em três eixos: territorial, de responsabilidade e de eficácia social. Nessa configuração, a parte final do texto não funciona como simples retomada conclusiva, mas como o espaço em que os achados teóricos e documentais são convertidos em critérios normativos de julgamento.

Ao final, a contribuição aferia é dupla. Em primeiro lugar, oferece uma leitura tecnicamente informada e juridicamente orientada sobre o videomonitoramento inteligente com leitura automática de placas veiculares em Pernambuco, evidenciando

a cadeia de decisões e os pontos críticos de governança. Em segundo lugar, propõe um enquadramento que permite avaliar a compatibilidade entre IA no policiamento e a democracia sem cair em respostas simplistas, mostrando que a discussão não se encerra na eficácia, mas depende de limites, controles e critérios públicos.

2 ESTRUTURA E DISCIPLINAMENTO DA VIGILÂNCIA DIGITAL

2.1 PERCURSO DA IMPLEMENTAÇÃO DO VIDEOMONITORAMENTO E DA INTELIGÊNCIA ARTIFICIAL

A compreensão do uso contemporâneo de câmeras ‘inteligentes’ com inteligência artificial (IA) exige situar o videomonitoramento em um percurso no qual a vigilância deixa de ser apenas captação e arquivamento de imagens e passa a incorporar camadas de interpretação automatizada do que é visto. Essa passagem não é meramente técnica: ela envolve novas formas de organizar a atenção, selecionar o que merece ser destacado e transformar o fluxo audiovisual em informação acionável. Estudos brasileiros sobre vigilância mostram que, nas redes contemporâneas, a videovigilância tende a operar como parte de uma “vigilância distribuída” (Bruno, 2012) e, no caso das câmeras inteligentes, como um sistema programado para detecção automatizada e em tempo real de situações consideradas irregulares ou suspeitas, com pretensão de antecipação e intervenção.

Antes da difusão das câmeras, já havia um imaginário e uma prática de vigilância estruturados por dispositivos humanos e institucionais — guardas, rondas, sentinelas e, sobretudo, mecanismos disciplinares que articulam observação, registro e correção. A leitura foucaultiana permite compreender que, desde o século XVIII, instituições como prisões, escolas e quartéis organizaram o controle por meio de regimes de visibilidade e de documentação, nos quais o ‘olhar’ funciona como técnica de governo das condutas (Foucault, 2014). A chegada do videomonitoramento não cria esse regime do nada; ela o intensifica e o reconfigura, deslocando progressivamente a observação do esforço humano contínuo para infraestruturas capazes de multiplicar pontos de vista, armazenar registros e, mais recentemente, classificar automaticamente o que aparece nas imagens — reforçando a passagem de uma vigilância centrada no observador para uma vigilância mediada por procedimentos técnicos.

Do ponto de vista histórico da técnica, uma referência recorrente para a gênese do circuito fechado de televisão (CFTV) é o seu uso em contexto militar, em pesquisa acadêmica sobre a história da televisão registra que, durante a Segunda Guerra, um circuito fechado foi construído e operado em *Peenemünde*, base de testes no nordeste da Alemanha, para controlar lançamentos dos foguetes V-2 (Tostes, 2013, p. 64). No

pós-guerra, a tecnologia migra gradualmente para usos civis e urbanos, e seu sentido passa a se vincular à gestão de fluxos, à prevenção situacional e à produção de registros para segurança. Em Pernambuco, esse deslocamento pode ser observado em estudos que identificam, já no ano de 2009, a criação do Centro Integrado de Operações de Defesa Social (CIODS) (Batista, 2013, p. 21) e a implantação de centenas de câmeras de vigilância eletrônica em bairros do Recife, como parte de uma estratégia de governo baseada em monitoramento e intervenção sobre espaços urbanos.

Nas décadas de 1960 e 1970, cidades como Londres começaram a instalar câmeras em vias públicas, estações de metrô e espaços de grande circulação, inicialmente para monitorar o trânsito e, depois, para apoiar a atividade policial (Lyon, 2003). Neste sentido Lyon (2003) destaca que, nesse período, o videomonitoramento ainda era visto como excepcional, um recurso ligado a situações específicas (grandes eventos, locais de risco, instituições financeiras). Aos poucos, porém, o uso se generaliza e as câmeras tornam-se parte da paisagem urbana, ao ponto de se tornarem quase invisíveis ao olhar cotidiano. No Brasil, o videomonitoramento começa a se expandir nos anos 1980, sobretudo em ambientes privados, como bancos, shoppings e edifícios comerciais. O objetivo era prevenir furtos, roubos e vandalismo, com gravações em fitas magnéticas revisadas a posteriori. A lógica era reativa: as imagens serviam como prova após o fato (Lemos *et al.*, 2011). Com o tempo, municípios passaram a instalar câmeras em pontos estratégicos de circulação, sobretudo em avenidas e cruzamentos, e a centralizar o acompanhamento das imagens em centrais de videomonitoramento. Nesse período, o funcionamento desses sistemas ainda dependia fortemente do trabalho contínuo de operadores e de uma infraestrutura técnica em consolidação (Bricalli, 2015, p. 64).

A transição do analógico para o digital, nas décadas de 1990 e 2000, altera de forma decisiva o papel do videomonitoramento. As câmeras deixam de gravar apenas em fitas locais e passam a transmitir imagens para centrais integradas, com armazenamento em servidores e, posteriormente, em nuvem (Kitchin, 2014).

Isso viabiliza a criação de redes de vigilância mais densas e distribuídas, em que diferentes órgãos públicos podem compartilhar imagens e informações. O vídeo torna-se dado passível de compressão, indexação, busca e cruzamento com outras bases informacionais.

É nesse momento histórico — entre o final da primeira metade do século XX e o início da era digital — que a inteligência artificial começa a se constituir como um campo teórico autônomo, capaz de dialogar com as práticas de automação, vigilância e gestão de informações visuais. Conforme observam Stuart Russell e Peter Norvig (2004, p. 27-33), as raízes conceituais da IA não estão apenas na engenharia, mas em um longo debate filosófico que atravessa as tradições da razão, da linguagem e da mente, temas centrais desde a Antiguidade. Assim, a ideia de uma máquina inteligente é, antes de tudo, uma questão sobre o que significa pensar, compreender e agir racionalmente.

Desde Aristóteles, a razão é vista como a faculdade que distingue o humano, vinculada à lógica e à capacidade de inferência (Aristóteles, 2005, p. 45-49). Séculos depois, com René Descartes, surge a concepção dualista de mente e corpo — uma cisão que abriria espaço para imaginar que a mente, sendo imaterial, poderia ser reproduzida ou simulada fora do corpo humano (Descartes, 1996, p. 58-65). No século XIX, pensadores como Leibniz e Boole formalizaram a ideia de que o raciocínio poderia ser traduzido em operações matemáticas, lançando as bases da lógica simbólica que, no século XX, alimentaria a arquitetura dos primeiros computadores (Boole, 1958, p. 1-3 e 23-25). No mesmo período, as reflexões sobre linguagem também se tornam decisivas. A filosofia da linguagem, de acordo com Ludwig Wittgenstein e o Círculo de Viena, introduz a noção de que o significado surge do uso e das relações estruturais entre símbolos — um princípio que ecoa nas tentativas da Inteligência Artificial (IA) de criar linguagens formais capazes de representar o mundo e instruir máquinas (Wittgenstein, 1999, p. 39-45). A inteligência, assim, passa a ser compreendida não apenas como um atributo interno do sujeito, mas como uma forma de ação simbólica mediada por sistemas de representação.

É nesse horizonte que emerge a figura de Alan Turing, cuja contribuição ultrapassa o domínio técnico e adentra o campo filosófico. Em seu célebre artigo ‘*Computing Machinery and Intelligence’,* publicado em 1950, Turing propõe uma ruptura: em vez de perguntar se as máquinas têm mente, ele sugere que se pergunte se elas podem se comportar de modo indistinguível de um ser humano em diálogo (Turing, 1950, p. 433-436). O que ficou conhecido como ‘Teste de Turing’ não busca sondar a interioridade da máquina, mas observar seus efeitos linguísticos, isto é, sua capacidade de simular o comportamento inteligente através da linguagem (Turing, 1950, p. 442-445).

Essa formulação desloca o problema da metafísica para a pragmática: o pensamento não é mais um privilégio ontológico, mas um processo verificável empiricamente por meio da interação comunicativa (Searle, 1980). Como explica Turing (1950), se uma máquina for capaz de sustentar uma conversação coerente, respondendo a perguntas de modo indistinguível de um humano, então ela deve ser considerada “pensante” no sentido funcional do termo. Tal definição inaugura o que Russell e Norvig (2004) chamam de abordagem comportamental da inteligência, base das pesquisas em agentes inteligentes e sistemas autônomos.

A proposta de Turing (1950) também antecipa questões éticas e epistemológicas ainda atuais: até que ponto a simulação equivale à compreensão? A linguagem é simples meio de comunicação ou expressão de consciência? John Searle (1980, p. 417-457), com seu experimento mental da “sala chinesa”, questionaria décadas depois se o processamento simbólico seria suficiente para gerar entendimento genuíno. Esse debate sobre inteligência sem consciência perpassa toda a história da IA e torna-se particularmente sensível quando aplicada à vigilância, pois a interpretação algorítmica de imagens e comportamentos reproduz decisões sem necessariamente compreendê-las em seu contexto humano.

Desse modo, a proposta de Turing (1950) não é apenas um marco técnico, mas uma fundação epistemológica da relação entre máquinas, linguagem e razão — fundamentos que hoje sustentam sistemas de IA capazes de identificar rostos, placas de veículos e padrões comportamentais nas cidades inteligentes. A ideia de que o comportamento observável pode servir como critério de inteligência ecoa diretamente no videomonitoramento automatizado, em que algoritmos “interpretam” sinais visuais e produzem inferências que substituem o olhar humano, materializando, na prática, a hipótese de Turing sobre o agir inteligente sem consciência.

A formalização da IA como disciplina ocorre na Conferência de Dartmouth, em 1956, quando pesquisadores como John McCarthy, Marvin Minsky e outros postulam que todos os aspectos da aprendizagem e da inteligência podem, em princípio, ser descritos de forma tão precisa que uma máquina poderia simulá-los (Russell; Norvig, 2004). A partir de então, desenvolvem-se programas capazes de resolver problemas matemáticos, jogar xadrez ou demonstrar teoremas lógicos, inaugurando a fase da chamada Inteligência Artificial (IA) simbólica, centrada em regras e representações explícitas de conhecimento (Russell; Norvig, 2004, p. 391-393).

Apesar do entusiasmo inicial, as limitações de *hardware*, a escassez de dados e a complexidade do mundo real conduzem a sucessivos períodos de frustração, conhecidos como “invernos da IA”, nos quais o financiamento e o interesse diminuem (Russell; Norvig, 2004, p. 1.105-1.107). Ainda assim, a área não desaparece, ela se reconfigura. Na década de 1980, os sistemas especialistas — programas baseados em regras de “se-então” codificadas a partir da expertise humana — voltam a conferir relevância à IA, sobretudo em domínios específicos como diagnóstico médico, finanças e controle industrial (Russell; Norvig, 2004, p. 29-30). Essa fase é importante porque inaugura a ideia de a IA auxiliar processos decisórios complexos, algo que mais tarde será aplicado ao campo da segurança pública.

A partir da década de 1990, a inteligência artificial passa por uma transformação metodológica decisiva que redefine suas bases epistemológicas e técnicas. Até então, a IA era predominantemente simbólica, isto é, dependente de regras lógicas e representações explícitas de conhecimento, elaboradas manualmente por programadores e especialistas. Esse modelo, também chamado de “boa e velha IA” (*Good Old-Fashioned Artificial Intelligence* – GOFAI), mostrava-se limitado diante da complexidade do mundo real, incapaz de lidar com a incerteza, a ambiguidade e o volume crescente de dados que caracterizavam a era digital nascente (Russell; Norvig, 2004, p. 27-33 e 861-864; Albino; Valente, 2023, p. 39-46).

Com o avanço do poder computacional e o aumento exponencial da capacidade de armazenamento de informações, surge uma nova abordagem centrada em métodos estatísticos e probabilísticos, conhecidos como aprendizado de máquina (*machine learning*) (Russell; Norvig, 2004, p. 59-63). Diferentemente dos sistemas simbólicos, que dependiam da codificação explícita de regras, o aprendizado de máquina permite que os sistemas aprendam por experiência, identificando padrões e correlações a partir da análise de grandes conjuntos de dados (Albino; Valente, 2023, p. 41-42). Esse deslocamento teórico e técnico significou uma mudança de paradigma: a ênfase deixa de estar na representação formal do raciocínio e passa a concentrar-se no ajuste adaptativo do comportamento da máquina em função dos exemplos recebidos.

Segundo Russell e Norvig (2004, p. 56-60), essa transformação marca o surgimento dos chamados “agentes que aprendem”, sistemas capazes de modificar suas ações com base na experiência acumulada, aprimorando sua *performance* a cada nova iteração. A IA deixa, assim, de ser um sistema rígido e determinístico,

tornando-se um processo dinâmico de aprendizado autônomo — uma virada que aproxima a tecnologia das formas biológicas de cognição. Essa mudança é também epistemológica, pois transfere a noção de inteligência de uma dimensão simbólica para uma dimensão empírica e estatística, em que o conhecimento emerge da própria manipulação de dados.

Essa evolução só se tornou possível graças à digitalização massiva dos registros humanos, fenômeno que Rob Kitchin (2014, p. 112-115) denomina de “[...] *datafication*: a conversão de aspectos da vida social em dados numéricos que podem ser armazenados, analisados e reutilizados”. Esse processo foi potencializado pela disseminação da *internet*, dos sensores digitais e, mais recentemente, das câmeras inteligentes — cuja produção de imagens contínuas e georreferenciadas alimenta diretamente sistemas de IA. O volume e a velocidade desses fluxos informacionais deram origem ao conceito de *big data*, caracterizado pelos “três Vs” — volume, variedade e velocidade — que definem a nova ecologia informacional das sociedades contemporâneas (Kitchin, 2014, p.68-70).

Do ponto de vista técnico, o *big data* fornece o substrato material necessário ao funcionamento dos algoritmos de aprendizado profundo, que dependem de vastos volumes de informação para atingir desempenho comparável ao humano (Russell, 2021, p. 181-182). Do ponto de vista político, entretanto, esse mesmo aparato inaugura novas formas de vigilância e controle social, uma vez que corporações e governos utilizam sistemas inteligentes para coletar, integrar e analisar dados sobre comunicações, deslocamentos e preferências individuais, produzindo perfis comportamentais detalhados da população (Russell, 2021, p. 2.015-2.016). A cada imagem capturada, deslocamento registrado ou transação processada, as máquinas “aprendem” a reconhecer padrões invisíveis ao olhar humano, transformando o cotidiano em fonte contínua de informação. Nesse contexto, como observa Zuboff (2019, p. 112-118), “[...] tudo o que pode ser convertido em dado, será”, sintetizando a lógica de captura total que estrutura o chamado capitalismo de vigilância.

Essa virada metodológica na IA impacta diretamente o campo do videomonitoramento, pois é o aprendizado de máquina que torna possível a análise automatizada de imagens e comportamentos em larga escala. Assim, câmeras conectadas passam a não apenas registrar, mas interpretar os eventos capturados — detectando movimentos anômalos, identificando placas de veículos, reconhecendo rostos e até inferindo emoções (Albino; Valente, 2023, p. 40-42). Deste modo, o

cruzamento entre IA e vigilância cria uma infraestrutura informacional que ultrapassa o olhar humano, operando em tempo real e com capacidade de decisão autônoma. O *big data*, portanto, não é apenas um insumo técnico, mas o elemento vital que sustenta a inteligência artificial enquanto ferramenta de vigilância e de gestão do espaço urbano.

Paralelamente, consolida-se a ideia de cidades conectadas e inteligentes, espaços urbanos nos quais infraestrutura física, redes de comunicação e sistemas de conhecimento são interligados para otimizar serviços e processos. Segundo estudos sobre cidades inteligentes no Brasil, essa integração tecnológica abrange sensores, bases de dados e redes de comando que permitem "[...] a coleta e análise de dados em tempo real para gerenciar recursos de maneira eficaz, facilitando a segurança pública" (Lazzaretti *et al*., 2019). Nesse contexto, o videomonitoramento deixa de funcionar como um conjunto de câmeras isoladas e passa a configurar-se como uma rede de observação distribuída — conectada a sensores, bancos de dados e centrais de comando — inserida no tecido urbano de forma permanente.

A noção de "dataficação", conforme tratada em estudos sobre cidades inteligentes e vigilância urbana, permite entender como atividades cotidianas — como o deslocamento de um carro, a caminhada em uma rua ou a entrada de um indivíduo em um edifício — passam a gerar dados passíveis de coleta, armazenamento e análise (Aguilar; Duque de Pinho, 2023). Nesse contexto, nas cidades inteligentes, cada veículo observado por câmeras, cada rosto detectado, cada trajeto registrado integra um fluxo contínuo de informação que pode ser utilizado para fins de gestão urbana, *marketing*, segurança ou controle social. A cidade e seus habitantes tornam-se, assim, em grande medida, legíveis para sistemas algorítmicos.

No Brasil, essa lógica ganhou força no contexto dos grandes eventos esportivos da década de 2010, quando a segurança pública passou a ser organizada por mecanismos extraordinários de coordenação e integração operacional entre diferentes órgãos. Em Pernambuco, esse movimento esteve diretamente ligado à preparação para a Copa do Mundo de 2014, pois desde o ano de 2012, a Assembleia Legislativa registrava a destinação de recursos para a implantação do Centro Integrado de Comando e Controle como estrutura de apoio ao evento, inserindo o Estado na agenda nacional de monitoramento e gestão integrada da segurança (ALEPE, 2012).

Mais recentemente, essa trajetória se projeta na renovação do sistema estadual de videomonitoramento, tanto pela instalação de duas mil câmeras digitais com inteligência artificial anunciada pela Secretaria de Defesa Social, quanto pelo novo processo licitatório, que prevê uma solução integrada de videomonitoramento de vias públicas com recursos de captação, transmissão, processamento, análise e gestão de eventos, incluindo leitura automática de placas (Pernambuco, 2024).

É nesse ponto que a IA deixa de ser apenas suporte e passa a "habitar" as câmeras. Técnicas de visão computacional, baseadas em redes neurais profundas (*deep learning*), são aplicadas ao fluxo de vídeo para detectar automaticamente eventos específicos: uma pessoa em atitude suspeita, uma aglomeração incomum, um veículo com placa cadastrada em base de interesse, um objeto abandonado (Albino; Valente, 2023, p. 49–50). O operador humano deixa de ser o único responsável pela seleção de cenas relevantes; essa triagem inicial passa a ser feita por algoritmos, que "sugerem" o que merece atenção prioritária.

Os sistemas de reconhecimento facial surgem nesse contexto como uma das aplicações mais controversas. Algoritmos treinados com grandes bases de imagens são capazes de identificar indivíduos em tempo real, comparando rostos capturados pelas câmeras com bancos de dados policiais ou administrativos. Estudos internacionais, porém, revelam que esses sistemas não são neutros, apresentando taxas de erro maiores para determinados grupos raciais e de gênero, o que levanta preocupações sobre discriminação algorítmica e reforço de seletividades já presentes no sistema de justiça criminal.

Outra aplicação diretamente ligada ao tema desta dissertação é o reconhecimento automático de placas veiculares (ANPR ou LPR) (Albino; Valente, 2023, p. 53-55). Esses sistemas capturam a imagem da placa, segmentam os caracteres, reconhecem-nos por reconhecimento óptico de caracteres (OCR) e os cruzam com bases de dados de veículos roubados, inadimplentes ou investigados. Em Pernambuco, a integração entre câmeras urbanas e sistemas de leitura de placas torna possível mapear, quase em tempo real, a circulação de veículos em rotas estratégicas, o que representa um ganho para investigações, mas também um aumento substancial da capacidade de rastreamento estatal.

A literatura de estudos de vigilância, especialmente em autores como Fernanda Bruno (2004, p. 37-39) e David Lyon (2003), destaca que essa passagem do videomonitoramento "reativo" para a vigilância preditiva altera o modo como o poder

se exerce. Em vez de apenas registrar um crime ocorrido, os sistemas procuram antecipar comportamentos considerados de risco, com base em padrões extraídos de dados históricos. Isso pode significar, por exemplo, maior concentração de atenção tecnológica sobre determinados bairros, horários ou perfis, reproduzindo desigualdades territoriais e sociais.

A inteligência artificial aplicada ao videomonitoramento não é um instrumento neutro. Ela reflete visões de mundo, escolhas de modelagem e prioridades políticas que orientam seus parâmetros de funcionamento. Ao automatizar decisões sobre quem observar, o que registrar e o que sinalizar como anômalo, esses sistemas passam a participar ativamente da produção de significados sobre ordem, risco e perigo no espaço urbano.

Nesse cenário, observa-se uma transição histórica que vai da vigilância visual localizada à vigilância algorítmica distribuída. O que antes se restringia a câmeras voltadas a espaços delimitados tornou-se uma infraestrutura complexa, formada por sistemas interconectados de vídeo, bancos de dados, inteligência artificial e redes de comunicação. Como analisa Silva (2020), o avanço dessas tecnologias consolida “[...] um regime de vigilância automatizado e contínuo, no qual o aprendizado de máquina e a visão computacional são atravessados por estruturas de poder e hierarquias raciais historicamente constituídas”. Trata-se de um fenômeno que dialoga com as leituras foucaultianas sobre disciplina e com as críticas contemporâneas ao capitalismo de vigilância, marcando a passagem de um poder centrado na observação para um poder exercido por meio da predição algorítmica. Esse panorama é essencial para compreender o uso contemporâneo de sistemas de IA em câmeras de vigilância no Estado de Pernambuco, pois evidencia que tais tecnologias resultam de um longo processo de sedimentação técnica e política da vigilância nas sociedades contemporâneas.

2.2 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E PROJETOS DE REGULAMENTAÇÃO NO BRASIL

A emergência de uma sociedade orientada por dados e tecnologias inteligentes colocou o direito brasileiro diante de uma encruzilhada: ou se atualizava para proteger a pessoa humana na esfera digital, ou assistiria, passivamente, à transformação do cidadão em mero objeto de coleta e exploração informacional. É nesse contexto que

se insere a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, resultado de um processo legislativo que buscou responder às demandas de um mundo marcado por fluxos transnacionais de informação e por práticas intensivas de vigilância tanto no setor privado quanto no poder público (Brasil, 2018).

A LGPD se apoia na ideia de que a proteção de dados pessoais está ligada à garantia de liberdades e direitos do titular, orientando o tratamento para finalidades legítimas e específicas e exigindo que a coleta e o uso sejam adequados e necessários ao propósito declarado (Brasil, 2018). Ao organizar esse regime por princípios como finalidade, adequação, necessidade, transparência, segurança e responsabilização, a lei busca impor limites práticos à coleta indiscriminada e condicionar qualquer tratamento a uma hipótese legal prevista e proporcional ao contexto. Com isso, procura-se reduzir o espaço para práticas de extração ampla e pouco transparente de informações, típicas de modelos econômicos baseados na transformação da experiência humana em dados para fins de previsão e influência comportamental (Zuboff, 2019, p. 19).

Um dos aspectos mais relevantes da Lei Geral de Proteção de Dados (LGPD) é o reconhecimento dos direitos dos titulares, entre os quais se incluem acesso, correção, portabilidade, anonimização, oposição e exclusão de dados, consoante os arts. 17 a 20 (Brasil, 2018). Esses direitos reforçam a ideia de autodeterminação informativa, concebida como a capacidade do indivíduo de decidir sobre o uso que é feito de suas informações pessoais. Tal noção dialoga diretamente com a tradição do direito europeu, principalmente com o Regulamento Geral de Proteção de Dados (GDPR), mas é transplantada para a realidade brasileira com a necessária adaptação institucional.

Ao mesmo tempo, a LGPD cria a Autoridade Nacional de Proteção de Dados (ANPD), responsável por orientar, fiscalizar e sancionar o tratamento de dados pessoais. Esse órgão tem papel estratégico na concretização da lei, pois é ele que estabelece regulamentações específicas, emite guias interpretativos e conduz processos administrativos, conforme Medida Provisória nº 869/2018 (Brasil, 2018). Sem uma autoridade forte e tecnicamente qualificada, o risco seria transformar a LGPD em uma carta de intenções sem efetividade prática, em face de grandes corporações tecnológicas e de políticas públicas baseadas em vigilância massiva.

Entretanto, a aplicação da LGPD encontra limitações importantes quando se trata de segurança pública, defesa nacional e atividades de investigação criminal.

Como dispõe o art. 4º da Lei nº 13.709/2018, a lei “[...] não se aplica ao tratamento de dados pessoais [...] realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou, d) atividades de investigação e repressão de infrações penais” (Brasil, 2018). Nesse ponto, a aproximação com Giorgio Agamben (2004, p. 15) mostra-se útil, pois, para o autor, o estado de exceção “[...] não é um direito especial [...], mas, enquanto suspensão da própria ordem jurídica”. Isso significa que o problema não reside apenas na existência de uma exclusão normativa, mas também no risco de abertura de um espaço de atuação estatal marcado por menor densidade de garantias, reduzida visibilidade pública e limitada capacidade de contestação. Nessa perspectiva, tecnologias como reconhecimento facial e videomonitoramento inteligente tendem a operar em um ambiente de controle jurídico enfraquecido, ampliando assimetrias de poder sobre os dados e sobre a própria vida urbana.

No plano doutrinário, autores brasileiros têm chamado atenção para esse descompasso. Neste sentido, Doneda e Monteiro (2021, p. 112-118), por exemplo, sustentam que a proteção de dados deve ser compreendida como expressão da dignidade da pessoa humana, inclusive — e talvez, sobretudo — em contextos de segurança pública. A ideia de que “quem nada deve, nada teme” não resiste a uma análise mais profunda: dados podem ser combinados, recontextualizados e utilizados para fins distintos daqueles que justificaram sua coleta, gerando perfis suspeitos, vieses discriminatórios e estigmatização de grupos vulneráveis.

Doneda e Monteiro (2021) desenvolvem, nesse sentido, uma teoria do consentimento informado relacional, em que a manifestação de vontade do titular dos dados não se reduz a um ato formal, mas constitui instrumento de autonomia substancial. O consentimento, quando compreendido apenas como requisito burocrático, não é suficiente para assegurar o controle efetivo do indivíduo sobre seus dados. Os autores defendem que ele deve ser inserido em um contexto de informação clara, previsibilidade e responsabilização, de modo a reequilibrar a relação entre os titulares e os agentes de tratamento. O foco desloca-se, portanto, da mera autorização para a governança participativa dos dados, em que a transparência e a confiança se tornam valores estruturantes da regulação.

A doutrina de Doneda e Monteiro (2021, p. 180-185) contribui ainda para uma leitura ética e institucional da proteção de dados. Os autores sustentam que o tratamento de informações pessoais envolve uma dimensão pública, pois a circulação

de dados afeta não apenas os indivíduos, mas a própria qualidade da vida democrática. Sob essa ótica, o direito à proteção de dados deixa de ser exclusivamente individual e passa a integrar o domínio dos direitos coletivos e difusos, constituindo um elemento essencial da cidadania informacional. Essa visão, que aproxima a proteção de dados das noções de *accountability* e solidariedade digital, reforça a compreensão da LGPD como instrumento de governança social e não apenas de regulação econômica.

Paralelamente à LGPD, o Brasil passou a discutir um marco regulatório específico para a inteligência artificial. O Projeto de Lei nº 2.338/2023, em tramitação no Senado Federal, disciplinando princípios, deveres e limites para o desenvolvimento e a aplicação de sistemas de IA no território nacional (Congresso Nacional, 2023). A proposta se inspira nas diretrizes internacionais sobre ética e governança algorítmica, notadamente no Regulamento Europeu de Inteligência Artificial (*AI Act*), e busca instituir um sistema de classificação de risco que diferencie usos ordinários de IA de aplicações potencialmente lesivas aos direitos fundamentais. Ao prever uma estrutura normativa de níveis de risco — mínimo, limitado, alto e inaceitável — o projeto incorpora o princípio da precaução tecnológica, que exige maior controle sobre tecnologias que possam afetar a privacidade, a liberdade e a igualdade (União Europeia , 2024).

O texto do Projeto de Lei nº 2.338/2023 reconhece que determinadas aplicações de IA, em especial as voltadas à segurança pública e ao monitoramento de espaços coletivos, exigem tratamento normativo mais rigoroso, conforme sua exposição de motivos (Congresso Nacional, 2023). Entre essas, destacam-se os sistemas capazes de identificar rostos humanos e placas de veículos em tempo real, utilizados em políticas de videomonitoramento urbano. A proposta legal considera que sistemas de reconhecimento facial e leitura automática de placas se enquadram na categoria de alto risco, por operarem em escala massiva e envolverem tratamento de dados sensíveis — particularmente dados biométricos, geográficos e de comportamento. O reconhecimento facial, por exemplo, é listado como tecnologia que pode afetar direitos à privacidade, à não discriminação e à presunção de inocência, demandando supervisão humana contínua, mecanismos de correção e auditorias independentes (Congresso Nacional, 2024).

No caso do reconhecimento facial, o Projeto de Lei nº 2.338/2023 menciona expressamente a necessidade de transparência algorítmica e explicabilidade das

decisões automatizadas, impondo obrigações ao desenvolvedor, ao fornecedor e ao operador do sistema (Congresso Nacional, 2023). O dispositivo prevê que toda tecnologia capaz de identificar pessoas deve permitir rastreabilidade das decisões, disponibilização de relatórios de impacto e documentação técnica sobre taxas de acerto, margem de erro e padrões de treinamento. A aplicação dessa exigência é particularmente relevante para os sistemas de vigilância urbana em Pernambuco, onde o uso de câmeras com IA tem se expandido para o reconhecimento automático de rostos e veículos em vias públicas e zonas de interesse policial (Diário de Pernambuco, 2020). Em tais contextos, a ausência de base legal específica e de protocolos padronizados pode resultar em práticas de monitoramento que extrapolam o princípio da necessidade previsto na Lei Geral de Proteção de Dados (LGPD) (Brasil, 2018).

O Projeto de Lei nº 2.338/2023 não trata expressamente dos sistemas de reconhecimento automatizado de placas veiculares (ANPR), mas estabelece um regime de governança aplicável a sistemas de inteligência artificial de alto risco utilizados pelo poder público, o que tende a abranger tais ferramentas quando integradas a bases de dados estatais e empregadas para fins de controle, investigação ou gestão pública. Nessa hipótese, a proposta legislativa exige protocolos de uso, rastreabilidade da atuação administrativa, garantias de explicação, revisão humana e avaliação prévia de impacto algorítmico. Nesse sentido:

> Art. 23 - Adicionalmente às medidas de governança estabelecidas neste Capítulo, todos os entes da Administração Pública direta e indireta, ao desenvolver ou utilizar sistemas de IA de alto risco, adotarão as seguintes medidas:
> I – definição de protocolos de acesso e de utilização do sistema que permitam o registro de quem o utilizou, para qual situação concreta e com qual finalidade;
> II – garantia facilitada e efetiva ao cidadão, perante o poder público, de direito à explicação e à revisão humanas de decisão por sistemas de IA que gerem efeitos jurídicos relevantes ou que impactem significativamente os interesses do afetado, a ser promovida pelo agente público competente;
> III – publicização em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos, das avaliações preliminares dos sistemas de IA de alto risco desenvolvidos, implementados ou utilizados pelo poder público da União, dos Estados, do Distrito Federal e dos Municípios.
> [...]
> Art. 25. A avaliação de impacto algorítmico de sistemas de IA é obrigação do desenvolvedor ou do aplicador que introduzir ou colocar sistema de IA em circulação no mercado, sempre que o sistema ou o seu uso forem de alto risco, considerando o papel e a participação do agente na cadeia.
> § 1º O desenvolvedor de sistema de IA de alto risco deverá [...] compartilhar com a autoridade setorial as avaliações preliminares e de impacto algorítmico, cuja metodologia considerará e registrará, ao menos, avaliação

> dos riscos e benefícios aos direitos fundamentais, medidas de atenuação e efetividade dessas medidas de gerenciamento (Congresso Nacional, 2023).

Em termos analíticos, isso significa que o eventual uso de ANPR pelo poder público deixa de ser tratado apenas como uma solução técnica de apoio operacional e passa a ser enquadrado por deveres de governança, documentação e controle. O ponto central não é apenas a captura automatizada de placas, mas a exigência de que sua utilização seja rastreável, justificável e submetida à avaliação prévia dos riscos que possam produzir sobre direitos fundamentais, principalmente quando houver cruzamento de dados, inferências automatizadas e efeitos relevantes sobre pessoas ou grupos afetados.

De acordo com os parâmetros do projeto, o uso de IA para o rastreamento automatizado de veículos e pessoas deve observar os princípios de finalidade legítima, minimização de dados e proporcionalidade (art. 5º, incisos X e XII da CF/1988) (Brasil, 1988). O tratamento massivo de dados biométricos e de circulação veicular, especialmente em ambientes urbanos densos, é reconhecido como uma das práticas mais intrusivas do ponto de vista da privacidade, exigindo contrapesos institucionais. Por isso, o Projeto de Lei nº 2.338/2023 recomenda que sistemas desse tipo contem com supervisão humana qualificada e mecanismos de revisão das decisões automatizadas, de modo que a atuação de agentes de segurança não se fundamente exclusivamente em inferências algorítmicas. No contexto pernambucano, tal diretriz é essencial, uma vez que o avanço dos sistemas de videomonitoramento inteligente tem ampliado a coleta e o cruzamento de dados entre órgãos públicos, demandando regras claras sobre interoperabilidade, retenção de informações e acesso às bases de dados.

A proposta também introduz o conceito de “governança responsável de IA”, que impõe obrigações às entidades públicas que utilizem algoritmos de vigilância, incluindo o dever de tornar públicos os critérios de funcionamento, os objetivos do sistema e os relatórios de conformidade (Congresso Nacional, 2022). Essa exigência se alinha às práticas internacionais de transparência em IA e reforça o controle social sobre o uso de tecnologias sensíveis. No caso de Pernambuco, a implementação de câmeras inteligentes interligadas à leitura de placas veiculares e à análise facial pode beneficiar-se dessas diretrizes, sobretudo no que se refere à padronização de protocolos de coleta e de retenção de dados. O projeto estabelece, ainda, que qualquer pessoa afetada por decisões automatizadas tem direito a requerer revisão

humana e acesso às informações sobre o tratamento de seus dados — ponto crucial para evitar arbitrariedades e consolidar a confiança pública em sistemas de segurança baseados em IA.

Essa movimentação legislativa evidencia o reconhecimento de que a LGPD, embora crucial, não é suficiente para dar conta de todos os desafios trazidos pela IA, sobretudo quando se trata de vigilância automatizada. Algoritmos que processam imagens de câmeras públicas, cruzam bases de dados e atribuem pontuações de risco a indivíduos ou territórios, operam em um nível de complexidade que exigem regras mais específicas, inclusive no que se refere à auditabilidade, ao combate a vieses e à possibilidade de contestação pelas pessoas afetadas.

Nesse cenário, a relação entre LGPD e projetos de regulamentação da IA precisa ser pensada em termos de complementaridade. A LGPD fornece o arcabouço geral de proteção de dados, assegurando princípios e direitos básicos; as leis específicas sobre IA podem detalhar obrigações adicionais para certos tipos de sistemas, como aqueles empregados em segurança pública, crédito, saúde e trabalho. A ausência dessa articulação poderia gerar lacunas normativas, nas quais a tecnologia avançaria mais rápido do que a capacidade regulatória do Estado.

2.3 EXPERIÊNCIAS INTERNACIONAIS: *AI ACT* E OUTROS MODELOS COMPARADOS

A discussão internacional sobre a regulação da inteligência artificial, especialmente quando acoplada a câmeras de vigilância e utilizada em investigações criminais, revela um movimento claro de reconhecimento do risco que essas tecnologias representam para direitos fundamentais. Em diversas jurisdições, a IA deixou de ser tratada apenas como tema de política de inovação para se tornar objeto central de debates constitucionais, de direitos humanos e de governança democrática. Esse contexto comparado é relevante para a reflexão sobre o uso de sistemas de IA em câmeras de vigilância no Estado de Pernambuco, pois indica parâmetros mínimos de proteção que vêm sendo adotados ou discutidos internacionalmente.

No âmbito da União Europeia, o ponto de referência mais importante é o Regulamento (UE) 2024/1689, conhecido como *Artificial Intelligence Act (AI Act)*, que estabelece regras harmonizadas para sistemas de IA em todos os Estados-Membros (União Europeia, 2024). O *AI Act* adota abordagem baseada em risco, classificando

os sistemas em categorias de risco mínimo, limitado, alto e inaceitável (União Europeia, 2024), as quais correspondem obrigações regulatórias diferenciadas. Essa estrutura tem como objetivo concentrar controles mais severos sobre aplicações que podem impactar de forma intensa direitos fundamentais, como ocorre justamente nos usos de IA para fins de segurança pública, identificação biométrica e investigação criminal.

Um dos aspectos mais sensíveis do *AI Act* para a temática desta dissertação é o tratamento dado aos sistemas de identificação biométrica remota em tempo real, em espaços de acesso público. Nesse regime, é importante distinguir juridicamente duas categorias. O risco elevado corresponde, em termos regulatórios, a situações em que a tecnologia pode ser admitida, mas apenas sob um conjunto reforçado de deveres, justamente porque apresenta maior potencial de afetar direitos fundamentais, exigindo governança e controle mais intensos. Por sua vez, o risco inaceitável é o patamar em que o próprio uso é considerado incompatível com a proteção de direitos, o que conduz à proibição como regra, admitindo-se somente exceções estritas e condicionadas (Bioni; Garrote; Guedes, 2023).

No caso da identificação biométrica remota em tempo real, por autoridades de segurança em espaços publicamente acessíveis, o *AI Act* a trata como prática proibida em regra, mas admite hipóteses excepcionais vinculadas a finalidades específicas e a salvaguardas rigorosas, como base legal, limites temporais e geográficos, autorização prévia por autoridade judicial ou independente e requisitos adicionais de avaliação de impacto e registro (União Europeia, 2024).

A lógica subjacente a essa disciplina é reconhecer que a combinação entre IA e câmeras de vigilância altera qualitativamente o poder de observação do Estado. A vigilância deixa de ser meramente reativa e localizada para se tornar proativa, contínua e automatizada, com capacidade de rastrear, identificar e correlacionar indivíduos em tempo real a partir de grandes bases de dados biométricos. Doutrina europeia recente tem advertido que, sem limites normativos rígidos, o uso policial de reconhecimento facial em espaços públicos tende a instaurar, na prática, uma forma de panoptismo digital incompatível com o Estado de Direito (Veale; Borgesius., 2021).

Além do *AI Act*, o arcabouço europeu inclui a Diretiva (UE) 2016/680, que regula o tratamento de dados pessoais por autoridades competentes para fins de prevenção, investigação, deteção ou repressão de infrações penais, e diretrizes específicas do Comité Europeu para a Proteção de Dados (EDPB) sobre o uso de reconhecimento

facial por autoridades de aplicação da lei. Esses instrumentos reforçam requisitos de finalidade determinada, proporcionalidade, necessidade, supervisão independente e limitação temporal e material no tratamento de dados biométricos (União Europeia, 2016). A lógica é impedir que tecnologias originalmente justificadas para cenários excepcionais se tornem soluções de vigilância generalizada na rotina das cidades.

Entre os marcos normativos mais recentes voltados à governança da inteligência artificial, destaca-se a Convenção-Quadro do Conselho da Europa sobre Inteligência Artificial, Direitos Humanos, Democracia e Estado de Direito, adotada em 2024, reconhecida como o primeiro tratado internacional juridicamente vinculante específico sobre IA. Conforme analisa Medeiros *et al*. (2023), a convenção representa um avanço substancial na tentativa de harmonizar os regimes regulatórios europeus e globais, estabelecendo obrigações para que os Estados assegurem a compatibilidade das atividades relacionadas à IA com os princípios de direitos humanos, democracia e Estado de Direito (Medeiros *et al.,* 2023) O texto prevê garantias como dignidade, autonomia individual, igualdade, transparência e supervisão humana, além de reconhecer que aplicações em contextos de segurança e justiça demandam salvaguardas reforçadas para prevenir discriminações e violações de direitos fundamentais.

Em nível multilateral, ganha destaque a Recomendação sobre a Ética da Inteligência Artificial, adotada pela Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), em 2021, atualizada em 2024, considerada o primeiro padrão global de ética em IA aprovado por 194 Estados-membros (UNESCO, 2021). Embora não possua força vinculante, o documento tem grande relevância política e simbólica ao afirmar que sistemas de IA não devem ser empregados para *social scoring* nem para vigilância em massa. Ao abordar o uso de tecnologias de reconhecimento facial e videomonitoramento, a Recomendação enfatiza os princípios da proporcionalidade, da não maleficência e da prestação de contas, exigindo que o uso de IA em segurança pública seja limitado, justificável e submetido a mecanismos de governança ética e transparência social (Lourenço; Silva, 2023).

Fora do contexto europeu, observa-se o esforço do Canadá em estruturar um marco regulatório próprio por meio do *Artificial Intelligence and Data Act (AIDA)*, integrante do Bill C-27 – *Digital Charter Implementation Act*. O projeto adota uma lógica de regulação baseada em riscos, centrada na categoria de “sistemas de alto impacto”, abrangendo aplicações capazes de afetar significativamente os direitos das

pessoas, como as utilizadas em vigilância e segurança pública (Gagnon; Péloquin, 2023) O AIDA prevê obrigações de gestão de risco, mitigação de danos e monitoramento de vieses, estabelecendo um modelo que combina inovação e responsabilização. Segundo Medeiros *et al*. (2023), a proposta canadense reforça a tendência de convergência global em torno de mecanismos de auditoria algorítmica e supervisão humana contínua, aproximando-se das diretrizes europeias e dos princípios éticos difundidos pela Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO).

A doutrina canadense aponta que em contextos de vigilância e investigação, tais como o uso de reconhecimento facial por forças policiais, a qualificação como “alto impacto” impõe deveres reforçados de auditoria, documentação e transparência (Canadá, 2023). Estudos empíricos demonstram que sistemas de reconhecimento facial tendem a apresentar taxas de erro mais elevadas para pessoas negras e outros grupos racializados, o que torna a regulação da discriminação algorítmica um ponto central (Buolamwini; Gebru, 2018). Nessa perspectiva, a abordagem canadense tende a alinhar a discussão de IA em segurança pública não apenas com a proteção da privacidade, mas também com o combate ao racismo estrutural e à seletividade penal.

No caso do Reino Unido, a regulação da inteligência artificial é estruturada a partir de instrumentos já existentes, em especial a Lei de Proteção de Dados, de 2018, e as orientações de 2020 sobre proteção de dados aplicadas à IA, as quais estabelecem princípios como responsabilidade e governança, tratamento justo, lícito e transparente, minimização e segurança de dados, bem como respeito aos direitos dos titulares. Nesse contexto, o *White Paper* lançado em abril de 2023 define cinco princípios fundamentais para orientar o uso e a regulação da inteligência artificial — segurança, transparência, responsabilidade, justiça e contestabilidade — e recomenda que tais princípios sejam adaptados por reguladores setoriais às especificidades de cada área, em vez de se adotar uma estrutura normativa única e rígida. Essa estratégia é descrita como uma abordagem “pro-inovação”, que busca equilibrar o estímulo ao empreendedorismo e ao teste de novas tecnologias, por meio de mecanismos como *sandboxes* regulatórios, com a proteção dos cidadãos e a prevenção de riscos excessivos (Medeiros *et al*., 2023).

Especificamente quanto ao uso de *live facial recognition* (LFR) por forças policiais, decisões judiciais e pareceres de órgãos de controle têm reconhecido a necessidade de limites e transparência, sem, contudo, estabelecer uma proibição

geral (Bridges, 2020). Na prática, isso resulta em uma regulação mais flexível, em que a admissibilidade da IA em câmeras de vigilância é avaliada à luz do cenário concreto e das salvaguardas implementadas. Esse arranjo tem sido criticado por organizações de direitos civis, que alegam falta de clareza sobre fronteiras materiais para o uso de LFR em manifestações, espaços públicos e investigações em larga escala, advertindo para o risco de normalização da vigilância algorítmica (Liberty; Big Brother Watch, 2002).

A experiência estadunidense apresenta um cenário distinto, marcado pela ausência, até o momento, de um marco federal abrangente sobre IA ou reconhecimento facial aplicado à segurança pública. A disciplina se encontra fragmentada entre normas de privacidade existentes, diretrizes administrativas e legislações estaduais ou municipais. Em algumas cidades, como São Francisco e outras jurisdições estadunidenses, foram aprovadas leis locais que proíbem ou restringem o uso de reconhecimento facial por órgãos públicos, justamente em razão de preocupações com privacidade e viés racial (Clark; Whitaker, 2023). Em outras, porém, a tecnologia vem sendo utilizada com pouca transparência, gerando controvérsias e litígios quanto à sua conformidade com direitos civis.

Nesse mosaico, organismos federais dos Estados Unidos têm emitido relatórios reconhecendo que o uso de IA e reconhecimento facial em investigações criminais exige atenção extraordinária a questões como acurácia, viés, possibilidade de contestação e risco de identificação errônea (USA, 2021). Ainda assim, a falta de um marco normativo coeso dificulta a criação de padrões mínimos de proteção em escala nacional, o que contrasta com a tendência europeia de harmonização legislativa. Essa disparidade evidencia que, na ausência de uma lei geral, a proteção de direitos em matéria de IA depende, em grande medida, da atuação de tribunais, da pressão da sociedade civil e de políticas internas de órgãos específicos.

A governança global da inteligência artificial tem se estruturado não apenas por instrumentos juridicamente vinculantes, mas também por mecanismos de *soft law*, cuja função é orientar políticas públicas e marcos regulatórios nacionais. A combinação entre normas obrigatórias (*hard law*) e diretrizes flexíveis (*soft law*) constitui estratégia essencial para equilibrar inovação tecnológica e proteção de direitos fundamentais (Medeiros *et al*., 2023). Essa abordagem, ao permitir adaptação a diferentes contextos, busca mitigar riscos e maximizar benefícios, promovendo práticas éticas e transparentes. Nesse sentido, a Organização para a Cooperação e

Desenvolvimento Econômico (OCDE) tornou-se referência com a adoção, no ano de 2019, dos “Princípios sobre Inteligência Artificial Confiável”, que estabelecem diretrizes voltadas à supervisão humana, robustez técnica, transparência, responsabilidade e inclusão social, atualizadas em 2024 para reforçar a cooperação internacional e o desenvolvimento de ecossistemas digitais inclusivos e sustentáveis (OECD, 2024).

Observa-se, portanto que as melhores práticas internacionais convergem em alguns pontos essenciais: (a) reconhecimento de que o uso de IA em câmeras de vigilância e investigações criminais é uma aplicação de alta sensibilidade, devendo ser tratada como de alto risco; (b) previsão de restrições materiais ou mesmo proibições a determinadas práticas, como identificação biométrica em tempo real em espaços públicos, salvo hipóteses excepcionais; (c) exigência de avaliações de impacto em direitos fundamentais, principalmente quando se trata de vigilância em larga escala; e, (d) imposição de deveres de transparência, supervisão humana e auditabilidade dos sistemas.

Em síntese, as experiências internacionais indicam que a IA aplicada à vigilância não é neutra, ela redistribui poderes, redefine prioridades investigativas e pode aprofundar seletividades já existentes. O caminho adotado por reguladores europeus, organismos internacionais e parte da doutrina comparada é o de submeter tais sistemas a um regime jurídico mais rigoroso, reconhecendo sua natureza de tecnologia de alto risco.

No contexto brasileiro, observa-se um movimento de aproximação às diretrizes internacionais de *soft law*, por meio da adoção de instrumentos como a Estratégia Brasileira de Inteligência Artificial (EBIA) e a tramitação do Projeto de Lei nº 2.338/2023, que institui o Marco Legal da Inteligência Artificial. Conforme analisam Medeiros *et al*. (2023), a EBIA estabelece eixos voltados à governança, ética e direitos humanos, além de estimular o uso responsável e transparente de tecnologias emergentes, buscando alinhar o país aos princípios da OCDE sobre IA confiável (*Ibidem*, 2023, p. 195-196). No que lhe concerne, o Projeto de Lei nº 2.338/2023, apresentado no Senado, propõe um modelo regulatório baseado em riscos, com distinção entre sistemas de alto, médio e baixo impacto, e prevê a obrigatoriedade de avaliações de impacto algorítmico e mecanismos de supervisão humana em aplicações sensíveis, como segurança pública e vigilância. Esse processo demonstra que o Brasil caminha para consolidar uma abordagem híbrida — combinando

elementos de regulação estatal e autorregulação orientada por princípios éticos — voltada à promoção da inovação tecnológica sem abdicar da proteção aos direitos fundamentais.

3 TEORIAS DO PANOPTISMO E DA VIGILÂNCIA CONTEMPORÂNEA

3.1 BENTHAM E FOUCAULT: PANOPTISMO, DISCIPLINA E VISIBILIDADE

A reflexão sobre o poder, a vigilância e o controle nas sociedades modernas encontram em Jeremy Bentham e Michel Foucault dois marcos teóricos decisivos. A ideia de que o olhar pode funcionar como instrumento de dominação, de organização social e de conformação subjetiva atravessa séculos e se atualiza nas mais diversas tecnologias de vigilância. Em Bentham, o olhar disciplinar nasce como um projeto arquitetônico racional, inspirado em princípios de economia e moralidade. Em Foucault, essa mesma estrutura é reinterpretada como um diagrama político, revelador das formas invisíveis de poder que constituem a modernidade.

O Panóptico, concebido por Jeremy Bentham no final do século XVIII, constitui um marco inicial para a reflexão sobre vigilância, disciplina e organização racional do espaço carcerário. Elaborado como resposta às condições de desordem, insalubridade e ineficácia que caracterizavam as prisões de sua época, o projeto buscava instituir um modelo arquitetônico capaz de tornar a inspeção contínua mais eficiente e econômica. Sua estrutura circular, com uma torre central de observação e celas distribuídas ao redor, permitia que os internos fossem potencialmente vistos a partir de um único ponto, sem jamais saber se estavam, de fato, sendo observados naquele momento. É precisamente dessa assimetria entre ver e ser visto que decorre a força disciplinar do dispositivo, como se percebe na seguinte formulação de Bentham (2008, p. 20):

> É óbvio que, em todos esses casos, quanto mais constantemente as pessoas a serem inspecionadas estiverem sob a vista das pessoas que devem inspecioná-las, mais perfeitamente o propósito do estabelecimento terá sido alcançado. A perfeição ideal, se esse fosse o objetivo, exigiria que cada pessoa estivesse realmente nessa condição, durante cada momento do tempo. Sendo isso impossível, a próxima coisa a ser desejada é que, em todo momento, ao ver razão para acreditar nisso e ao não ver a possibilidade contrária, ele deveria pensar que está nessa condição.

Essa incerteza é o que garante o efeito disciplinar do modelo. Para Bentham, não era necessário que o observador estivesse sempre atento — bastava que os prisioneiros acreditassem que poderiam estar sob vigilância a qualquer momento (Bentham, 2008, p. 22-25). A visibilidade contínua transformava-se, assim, em um

meio de controle psíquico: o medo de ser visto fazia com que cada indivíduo se comportasse de acordo com as normas esperadas, mesmo na ausência de coerção direta.

O Panóptico opera, portanto, como uma tecnologia de poder fundada na assimetria do olhar: o vigilante vê sem ser visto, enquanto o vigiado se expõe sem jamais ter certeza de que está efetivamente sob observação. É justamente essa incerteza que assegura a eficácia do dispositivo, pois, como afirma Bentham (2008, p. 20), “[...] a próxima coisa a ser desejada é que, em todo momento, ao ver razão para acreditar nisso e ao não ver a possibilidade contrária, ele deveria pensar que está nessa condição”. A luz desempenha papel decisivo nesse arranjo, as celas devem ser iluminadas e transparentes, ao passo que a torre central permanece resguardada pela sombra. Essa distribuição desigual da visibilidade converte a arquitetura em mecanismo disciplinar. Para Bentham, contudo, o Panóptico não se limitava ao espaço prisional, mas constituía um princípio mais amplo de organização social, passível de aplicação a hospitais, escolas, fábricas e casas de correção. A proposta revela, assim, seu caráter utilitarista de substituir a coerção física por uma vigilância contínua, racionalizada e potencialmente interiorizada pelos próprios indivíduos.

Na leitura de Gonçalves (2003, p. 49-56), o Panóptico é uma “tradução arquitetônica do ideal utilitarista de Bentham”, no qual a economia de recursos coincide com a moralização dos costumes. Em outras palavras, o dispositivo não se limita a punir; ele educa, corrige e normaliza. O espaço arquitetônico torna-se um meio pedagógico e político de formação de sujeitos úteis à ordem social.

No entanto, a promessa de transparência e racionalidade do Panóptico também contém uma dimensão de ambiguidade. Ao propor uma estrutura na qual poucos controlam muitos, Bentham cria, inadvertidamente, um modelo de poder absoluto, no qual a opacidade do observador é condição da docilidade dos observados Trindade, 2011, p. 251-255). Essa assimetria é o que despertará, dois séculos depois, a atenção crítica de Michel Foucault.

Em Vigiar e Punir, Foucault recupera o Panóptico para analisá-lo não como invenção isolada, mas como símbolo de uma nova racionalidade política (Foucault, 1999, p. 189-215). O filósofo francês desloca o foco da arquitetura para o que ela representa: um modo de exercício do poder que se difunde silenciosamente pelas instituições modernas. O Panoptismo, em sua leitura, não é apenas uma técnica de

observação, mas um diagrama de poder — uma lógica que articula vigilância, normalização e produção de saberes (Foucault, 1999, p. 115-135).

Foucault (1999) situa o Panóptico no contexto da passagem das sociedades do suplício para as sociedades disciplinares. Nas antigas formas de punição, o castigo era público, corporal e espetacular, o soberano demonstrava sua força sobre o corpo do condenado. Com o advento das disciplinas, esse poder se interioriza. A punição se desloca do corpo para a alma; o castigo visível é substituído pelo olhar invisível. A prisão panóptica simboliza essa mudança: não se trata mais de destruir o corpo do infrator, mas de observar, corrigir e reformar sua conduta. Doravante, o indivíduo passa a ser objeto de registros, relatórios e classificações (Foucault, 2012, p. 209-228). O poder se infiltra nas minúcias da vida cotidiana, administrando o tempo, o espaço e o comportamento.

Ao reinterpretar Bentham, Foucault propõe uma teoria do poder disciplinar — um poder que produz corpos úteis e dóceis. O Panoptismo é o modelo ideal dessa racionalidade, pois permite que o controle se torne automático e internalizado (Sousa. Menezes, 2010). O sujeito, ciente de que pode ser observado, passa a vigiar a si mesmo. Assim, o olhar externo transforma-se em autovigilância, e o poder, antes repressivo, converte-se em produtivo.

Em lugar de compreender o poder apenas como proibição ou repressão, a perspectiva foucaultiana evidencia seu caráter produtivo, ele fabrica subjetividades ao articular vigilância, exame e normalização. O olhar institucional — distribuído entre dispositivos como prontuários, relatórios, estatísticas e avaliações — não só controla condutas, como define parâmetros do “normal”, “saudável” e “útil”, constituindo sujeitos que se reconhecem à luz desses saberes. O “sujeito moderno”, nessa chave, é efeito de uma trama contínua de observações e classificações que atravessam escola, fábrica, hospital e prisão, onde a disciplina se infiltra no corpo e na alma como técnica cotidiana de governo (Teixeira, 2006, p. 17-33[2]).

A autora Daniela Pessanha Teixeira (2006) enfatiza que em Foucault, o poder opera como relação e como “ações sobre ações”, deslocando o foco de centros soberanos para as práticas capilares que incidem sobre os corpos e os hábitos. É nesse plano micropolítico que se compreende a fórmula segundo a qual o indivíduo

[2] Recomenda-se a leitura de Teixeira (2006), sobretudo no que concerne ao capítulo intitulado ‘Corpo, poder e formas de subjetivação em Foucault’ - especialmente seções 2.1 e 2.2, onde a autora discute a relação saber-poder, disciplina e constituição da subjetividade.

não é o contraponto do poder, mas “um de seus efeitos primeiros”, a subjetividade constitui-se no entrelaçamento de saberes e práticas que nomeiam, examinam, corrigem e tornam visíveis condutas e identidades. Ao privilegiar a articulação “corpo-alma-poder”, Teixeira (2006) mostra como a disciplina se converte em tecnologia de subjetivação, sustentada por técnicas de registro e exame que conferem inteligibilidade e governabilidade à experiência individual.

Nesse horizonte, a tríade vigilância–exame–normalização funciona como mecanismo de produção de verdade sobre os sujeitos. Cada prontuário, laudo ou avaliação integra uma economia de saber-poder que define pertencimentos e desvios, autorizando intervenções pedagógicas, médicas, penais e administrativas. Em diálogo com Vigiar e Punir, pode-se dizer que os “corpos dóceis” resultam dessa gramática de visibilidade e correção contínua, na qual o Panoptismo é menos um edifício e mais um diagrama que organiza práticas institucionais (Foucault, 1999; Candiotto, 2012[3])

Na leitura de Sousa e Meneses (2010, p. 18–22), o Panoptismo em Foucault não se reduz a um edifício prisional, mas opera como princípio organizador da sociedade moderna, uma tecnologia política que reconfigura instituições e condutas ao transformar a visibilidade em técnica de governo. O “ver sem ser visto” torna-se método difuso de disciplina. Por meio de vigilância, exame e registro, instauram-se rotinas de classificação e normalização que atravessam escola, hospital, fábrica e prisão, produzindo sujeitos ajustados a padrões de utilidade e docilidade. O Panoptismo, assim, descreve uma economia do olhar que articula saber e poder — os dispositivos de observação geram conhecimentos (prontuários, relatórios, estatísticas) que legitimam intervenções corretivas, enquanto essas intervenções reforçam a própria ordem visual que as sustenta. Em termos foucaultianos, trata-se de uma microfísica capilar do poder que abandona o suplício espetacular em favor de uma administração contínua da conduta, na qual o indivíduo é simultaneamente objeto de observação e efeito das práticas que o tornam visível.

O alcance do Panoptismo ultrapassa o espaço prisional. Escolas, hospitais, quartéis e fábricas tornam-se microcosmos panópticos, onde a vigilância é contínua e os comportamentos são regulados por normas minuciosas. Cada instituição reproduz o mesmo princípio: organizar o espaço, individualizar os sujeitos e permitir a observação constante (Oliveira, 2016).

[3] Recomenda-se a leitura: Foucault (1999, p. 135-169 e p. 189-215) e Candiotto (2012, p. 18-24).

A análise foucaultiana mostra que o poder disciplinar é inseparável da produção de saberes (Siqueira, 2013). A vigilância não apenas observa, ela registra e arquiva. Prontuários, dossiês e estatísticas transformam o olhar em informação (Bruno, 2018, p. 15-20, 40-43 e 90). O conhecimento gerado pela observação legitima novas formas de poder, num ciclo em que saber e controle se reforçam mutuamente (Foucault, 2008, p. 11-14).

Foucault (2008, p. 26-27) enfatiza ainda que o poder disciplinar não precisa de violência para se impor. Ele atua na sutileza dos gestos, na repetição das práticas e na interiorização das normas. Por isso, o Panoptismo é mais eficaz quanto mais invisível. Ou seja, o ideal não é o terror, mas a previsibilidade; não o castigo, mas o adestramento.

Autores brasileiros têm mostrado que, em Foucault, o “olhar” institucional desempenha uma dupla função intimamente articulada: de um lado, é instrumento de produção de saber — isto é, um operador epistemológico que coleta, organiza e valida informações sobre os corpos por meio de exames, prontuários, relatórios e classificações; de outro, é mecanismo de sujeição — um operador político que normaliza condutas, induz autovigilância e fabrica subjetividades ajustadas a padrões de utilidade e docilidade. Nessa chave, o indivíduo não apenas é observado, medido e avaliado, ele também se reconhece à luz desses dispositivos, reconfigurando a própria identidade a partir das categorias que o nomeiam e situam (normal/anormal, apto/inapto, saudável/doente, delinquente/reabilitado). O “olhar” foucaultiano, portanto, não se limita a registrar uma realidade dada. Ele constrói a realidade social por meio de práticas de visibilidade que tornam o sujeito governável, convertendo conhecimento em poder e poder em conhecimento, um circuito no qual as técnicas de exame e registro, ao mesmo tempo que disciplinam corpos, constituem identidades e subjetividades no interior de escolas, hospitais, fábricas e prisões (Teixeira; Caminha; Lima Neto, 2017).

Quando confrontados, Bentham e Foucault revelam abordagens distintas, mas complementares. Bentham descreve o Panóptico como uma utopia racional, uma promessa de eficiência e moralização. Foucault o reconstrói como paradigma crítico, uma metáfora das novas formas de poder que atravessam o tecido social.

A diferença entre Bentham e Foucault não é apenas histórica, mas normativa e política. Enquanto o projeto benthamiano apresenta a vigilância como virtude racional, um arranjo eficiente de reforma moral que economiza recursos e promove ordem, a

leitura foucaultiana revela a vigilância como técnica de dominação que se naturaliza nas práticas cotidianas, operando por persuasão, normalização e autovigilância. Em outras palavras, o que em Bentham é arquitetura de “inspeção” virtuosa, em Foucault é diagrama de poder que organiza condutas e fabrica sujeitos (Oliveira; Carneiro, 2016, p. 101-116).

A partir dessa chave, o Panoptismo deixa de ser um conceito restrito às prisões para tornar-se categoria interpretativa da modernidade, pois sua lógica atravessa instituições e dispositivos, atualizando-se nos sistemas de videomonitoramento urbano, nas plataformas digitais e nos bancos de dados que classificam e preveem comportamentos. Assim como o observador panóptico, algoritmos e infraestruturas de dados fazem ver (e registrar) sem serem vistos, convertendo a visibilidade em instrumento de governo. Estudos brasileiros sobre visibilidade e subjetividade mostram como, nesse cenário, o “olhar” técnico alimenta saberes, padrões e intervenções normativas (Bruno, 2004).

Desse modo, o diálogo entre Bentham e Foucault permanece central para compreender como a vigilância é naturalizada e incorporada à vida social. A arquitetura do olhar, seja no edifício circular do século XVIII ou nas redes informacionais do século XXI, funciona como meio privilegiado de governo, uma vez que ver, registrar e correlacionar dados não apenas descreve a realidade, mas a conforma de acordo com matrizes de utilidade, eficiência e risco. Pesquisas recentes em psicologia política e comunicação reforçam esse ponto ao examinar a economia visual do poder e seus efeitos de subjetivação (Santos; Portugal, 2019).

Examinar as origens e as transformações do Panoptismo evidencia que a vigilância moderna se sustenta tanto na capacidade de observar quanto na produção de subjetividades conformes. O poder não é somente aquilo que vigia; é também aquilo que ensina a ser visto e que orienta o indivíduo a ver-se como objeto governável — por exames, *rankings*, prontuários e métricas. Essa dupla operação (epistemológica e política) estrutura o nexo entre saber e poder que Foucault situa no centro das instituições modernas (Sousa; Meneses, 2010).

3.2 DO PANOPTISMO À SOCIEDADE DE CONTROLE: DELEUZE E O PODER EM REDE

A releitura deleuzeana da vigilância parte do diagnóstico de que as instituições disciplinares descritas por Foucault — prisão, fábrica, escola, hospital — já não esgotam o entendimento do poder contemporâneo. Em seu '*Post-scriptum* sobre as sociedades de controle', Deleuze (1992) propõe que o eixo do poder se desloca do confinamento institucional para mecanismos contínuos de modulação, operando por códigos, senhas e bancos de dados que atravessam todo o tecido social.

Em vez do espaço fechado da instituição, o ambiente aberto e informatizado torna-se o lugar privilegiado do controle. Não se trata de abolir a disciplina, mas de reconfigurá-la em redes que conectam pontos e fluxos: cartões magnéticos, sistemas de crédito, plataformas digitais e registros eletrônicos compõem uma malha na qual o poder age sem precisar da clausura visível das antigas arquiteturas (Costa, 2004).

Em Deleuze (1992), a transição das sociedades disciplinares às sociedades de controle desloca o foco do confinamento institucional para a modulação contínua por códigos, senhas e bancos de dados; em lugar do "homem confinado", emerge o homem endividado, cuja circulação é gerida por mecanismos informatizados que acompanham e ajustam condutas em tempo real. Para designar a segmentação e recombinação de perfis em ambientes digitais, parte da literatura brasileira adota a noção de "dividual", enfatizando que identidades são tratadas como conjuntos de traços e probabilidades mobilizados por plataformas e dispositivos de vigilância distribuída (Rodriguez, 2015).

A passagem do Panoptismo à sociedade de controle pode ser descrita como mudança do modelo espacial para o modelo reticular, pois o poder já não se concentra numa torre que tudo vê, mas se distribui por sensores, bases de dados e algoritmos que classificam e preveem comportamentos. O olhar torna-se infraestrutural, indissociável das redes de comunicação que organizam circulação, crédito, informação e mobilidade (Peron, 2018).

A literatura brasileira sublinha que essa transição não implica simples substituição de um regime por outro, e sim uma superposição histórica, porque práticas disciplinares persistem, mas são englobadas pelas lógicas de controle distribuído. Em termos deleuzeanos, a modulação substitui o molde; a norma dá lugar a curvas de ajuste contínuo que operam em tempo real (Costa, 2004).

Uma consequência decisiva do controle reticular é a centralidade dos dados. A captação, o armazenamento e o cruzamento massivo de informações passam a orientar decisões de segurança, crédito, saúde, publicidade e governo. Na vigilância contemporânea, a ênfase desloca-se do sujeito corporal para o rastro informacional que ele deixa ao usar serviços e dispositivos (Lott; Cianconi, 2018).

Essa reconfiguração faz com que a vigilância deixe de ser uma prática apenas "externa" e passe a ser parte da cultura, segundo análises recentes, hábitos de autocontabilização, monitoramento voluntário e exposição contínua ampliam o alcance do controle sem romper com a retórica da liberdade individual e da conveniência (Bricalli, 2020).

No policiamento e na segurança pública, o paradigma de controle se materializa em plataformas analíticas que articulam registros administrativos, dados de mobilidade, imagens e metadados. O foco não está apenas no infrator individual, mas em padrões extraídos de grandes bases, capazes de orientar ações preventivas, alocação de recursos e definição de "zonas quentes" (NEV, 2023).

Deleuze (1992) aponta que o capitalismo contemporâneo requer flexibilidade, endividamento e formação permanente. Em lugar do trabalhador preso a um posto fixo, multiplicam-se avaliações, certificações e atualizações contínuas. O controle torna-se uma avaliação sem fim, na qual cada interação retroalimenta o cálculo sobre o que se pode permitir, negar ou tarifar.

Na educação, observa-se a passagem de um regime de avaliações episódicas (provas/exames em datas fixas) para um monitoramento contínuo de desempenho mediado por plataformas: ambientes virtuais de aprendizagem registram tempo de acesso, taxa de conclusão de tarefas, participação em fóruns e resultados de *quizzes*; *dashboards* convertem essas ações em indicadores que retroalimentam regras de progressão, recomendação de conteúdo e, por vezes, incentivos disciplinares. Na chave deleuzeana, trata-se da substituição do "molde" (exame pontual) pela "modulação" (ajuste permanente), em que códigos e senhas mediam o acesso a recursos, atividades e certificações. Essas métricas funcionam como chaves de passagem: abrem ou fecham portas acadêmicas (pré-requisitos, trilhas de estudo, abertura de módulos) a partir do comportamento capturado pela própria plataforma. Estudos nacionais associam esse movimento à "sociedade de controle", na qual a avaliação se torna processamento contínuo de dados e o governo das condutas

ocorre por *feedbacks* algorítmicos que recompensam a aderência a padrões de engajamento (Deleuze, 1992).

No campo educacional, esse processo se manifesta na substituição de avaliações concentradas em momentos específicos por formas permanentes de acompanhamento do desempenho estudantil.

Por sua vez, no trabalho e no consumo, a lógica de pontuação e ranqueamento estrutura oportunidades de crédito, emprego, contratação de serviços e visibilidade em plataformas (*scores* de crédito, reputação de motoristas/entregadores, índices de risco, *ratings* de vendedores). Em vez de um sujeito fixo avaliado por um exame único, emerge o perfil segmentado e recombinável a partir de traços quantificáveis (histórico de pagamentos, geolocalização, redes de contato, comportamento transacional). Parte da literatura denomina essa figura de “dividual”, salientando que identidades se tornam conjuntos de dados acionados segundo regras de decisão que distribuem direitos e oportunidades de modo diferencial (limites, juros, prazos, ofertas, tarifas). Pesquisas brasileiras mostram que esses arranjos ampliam assimetrias informacionais e podem tensionar garantias como autodeterminação informativa e não discriminação, especialmente quando critérios e pesos dos modelos permanecem opacos ao público (Rodriguez, 2015; Siqueira, 2023).

Do ponto de vista infraestrutural, a vigilância contemporânea está cada vez mais algorítmica: mineração de dados, perfilização geográfica (*geo-profiling*), correlação de metadados e classificação automatizada operam como verdadeiros diagramas de força, articulando saber e poder por meio do cálculo. Nesses ambientes, o problema central deixa de ser apenas “quem vê”, para se tornar “quem computa o quê, com quais dados e segundo quais parâmetros”. Relatórios e artigos brasileiros documentam a convergência entre bases administrativas, imagens e registros de mobilidade em plataformas analíticas que antecipam condutas (previsão de demanda/risco, segmentação territorial, definição de prioridades), deslocando a vigilância do olhar para o processamento e da prova singular para a probabilidade (Peron, 2018; Lott; Cianconi, 2018).

Nessa perspectiva, a metáfora da torre panóptica cede lugar a formas reticulares e distribuídas de vigilância mais próximas da nuvem, do grafo e dos fluxos de dados do que da arquitetura disciplinar clássica. O controle já não depende apenas de um ponto fixo de observação, mas de cadeias técnicas de captura, processamento e circulação informacional mediadas por plataformas, interfaces e APIs pouco

transparentes. Como observa Fernanda Bruno (2013, p. 81), na videovigilância contemporânea, “[...] o sujeito do olhar da câmera é, antes de tudo, invisível, desconhecido e inverificável por parte dos que são observados”. Essa formulação ajuda a compreender que a assimetria entre saber e poder se desloca da visibilidade arquitetônica do Panoptismo para a opacidade algorítmica dos sistemas atuais, nos quais os critérios de classificação, correlação e decisão raramente se tornam plenamente auditáveis. O próprio trecho que você já tem no arquivo está apoiado nessa referência.

A crítica deleuzeana ajuda a compreender por que a vigilância digital se mantém eficaz sem a presença de um soberano visível. Ela se confunde com a própria infraestrutura de vida — pagamentos, mobilidade, comunicação, serviços públicos e privados —, em que cada acesso depende de credenciais e cada ação deixa traços que realimentam os modelos de decisão.

A noção de controle como modulação explica também a escalabilidade do poder nas plataformas. Pequenas mudanças de parâmetros em sistemas de recomendação, ranqueamento ou detecção geram grandes efeitos populacionais, distribuindo visibilidade, atenção e recursos. Trata-se de um governo por meios técnicos de alcance difuso, difícil de localizar e responsabilizar (Corbanezi,' 2019).

Estudos recentes falam em sociedade de controle algorítmica, destacando que a extração contínua de dados, combinada a modelos de aprendizado de máquina, produz sujeitos calculáveis, ajustados por *feedbacks* invisíveis. Não é apenas o indivíduo que muda de comportamento porque “pode estar sendo visto”, mas porque o ambiente muda ao seu redor em resposta às previsões e classificações (Corrêa; Macías, 2020).

Essa dinâmica implica uma forma de governo das condutas que opera menos pela interdição explícita e mais pela modulação das condições de possibilidade. Recomendações, ranqueamentos, limiares de acesso, alertas e filtros reconfiguram o campo de ação antes mesmo que o sujeito delibere, deslocando a coerção do gesto visível para a arquitetura discreta do sistema. Nessa ambiência, o controle se exerce como administração probabilística do futuro, na medida em que decisões presentes passam a ser justificadas por inferências sobre comportamentos esperados, convertendo previsões em critérios práticos de intervenção. O efeito é a estabilização de uma subjetividade “calculável”, cuja legibilidade depende de métricas e rastros, cuja autonomia é tensionada por mecanismos que ajustam o entorno conforme perfis

e padrões atribuídos. Assim, a vigilância algorítmica não apenas observa o social, ela o produz performativamente, porque as classificações retroagem sobre os próprios fenômenos que dizem descrever, reforçando trajetórias, distribuindo suspeição e redefinindo o que conta como normal, seguro ou aceitável em cada contexto.

Esse cenário repercute na autonomia e na cidadania informacional uma vez que os critérios que definem acesso, risco e prioridade são inscritos em código e atualizados em velocidade superior à capacidade de escrutínio público (Elesbão, 2020). A promessa de eficiência convive com riscos de discriminação estatística, viés e opacidade decisória.

Do ponto de vista metodológico, Deleuze propõe deslocar a análise do *molde* institucional para a modulação em meios abertos, regida por senhas/códigos e processamentos contínuos de informação; não se trata apenas de prisões, fábricas e escolas como espaços fechados, mas de ambientes reticulares onde o poder atua distribuído por interfaces, credenciais e bancos de dados.

A leitura brasileira de Rogério da Costa explicita esse movimento ao caracterizar a sociedade de controle como uma governamentalidade em rede, na qual a avaliação permanente e a circulação informatizada substituem os confinamentos típicos das disciplinas (Costa, 2004). Essa leitura converge com os estudos de vigilância que, no Brasil, têm enfatizado a passagem da vigilância “sobre corpos” para vigilância mediada por dados, sem perder de vista o entrelaçamento com práticas policiais, financeiras e mercadológicas. Ao substituir o “olhar” pelo “cálculo”, o controle reticular redobra a atualidade crítica do diagnóstico deleuziano (Duarte; Nunes; Lima, 2023, p. 5-8 e 41-42).

Importa sublinhar que a sociedade de controle não descreve um futuro distante, mas um presente operativo: autenticações contínuas, *scoring*, análise de trajetórias, monitoramento por dispositivos móveis, sensores urbanos e plataformas de serviços compõem um clima técnico no qual “viver” e “ser governado” tornam-se dimensões difíceis de separar.

A vigilância, nesse contexto, é menos um ato excepcional de observação e mais uma condição de funcionamento de sistemas sociotécnicos que prometem conveniência e segurança. O que Deleuze chama de “controle” é, em suma, a capacidade de modular comportamentos por meio de infraestruturas que aprendem com os dados que coletam e, por isso mesmo, ajustam continuamente as possibilidades de ação.

Por fim, o deslocamento do Panoptismo ao controle não autoriza concluir que as críticas à disciplina perderam validade, ao contrário, elas se rearticulam. A questão deixa de ser apenas “quem vê quem”, para tornar-se também “quem calcula o quê, com quais dados, segundo quais normas”. Ao trazer o poder em rede para o centro da análise, a proposta deleuzeana fornece instrumentos para pensar a regulação democrática de plataformas, algoritmos e bases de dados, e para recolocar a política no coração da técnica.

3.3 VIGILÂNCIA DIGITAL, CAPITALISMO DE DADOS E SUBJETIVAÇÃO CONTEMPORÂNEA

No século XXI, Byung-Chul Han propõe que a sociedade disciplinar descrita por Foucault cede lugar a uma sociedade da transparência, na qual a coerção direta é substituída pela lógica da autoexposição voluntária. Em vez de um olhar imposto de fora, passa a prevalecer um regime em que os indivíduos se exibem espontaneamente, sobretudo nas redes sociais e ambientes digitais (Han, 2017, p. 29-36). O ‘panóptico’ já não depende de uma torre central, ele se reproduz nas telas dos dispositivos móveis, nos perfis pessoais, nos *likes* e nos rastros digitais deixados em cada interação.

Nas leituras contemporâneas de Byung-Chul Han (2017), o sujeito é descrito como um “empreendedor de si”, cuja vida passa a ser organizada segundo a lógica do desempenho e da autoexploração. Em vez de se constituir como alvo de uma vigilância externa e coercitiva, esse sujeito se engaja ativamente em práticas de exposição de si, transformando a própria experiência em objeto de gestão, otimização e consumo simbólico (Trigueiro; Costa, 2023, p. 41-57). A vigilância assume, assim, formas sedutoras, associadas a promessas de visibilidade, reconhecimento e pertencimento, de modo que mecanismos de controle se apresentam como escolhas individuais e oportunidades de realização pessoal (Rodrigues, 2022). Nesse quadro, a fronteira entre liberdade e controle torna-se difusa, dispositivos digitais de monitoramento e circulação de dados produzem um “panóptico” interiorizado em que o indivíduo colabora com os mesmos sistemas que o observam e o perfuram como perfil, sob um regime contínuo de autoavaliação e cobrança (Viana, 2023).

É nesse ponto que a teoria da vigilância contemporânea dialoga diretamente com o avanço das tecnologias digitais. A integração entre câmeras, bancos de dados,

sensores urbanos e sistemas de inteligência artificial cria uma espécie de panoptismo algorítmico, em que o olhar humano é substituído por operações automáticas de captura, análise e previsão de comportamentos. Autores como David Lyon e Shoshana Zuboff mostram como o cotidiano passa a ser “dataficado”, ou seja, traduzido em dados que podem ser comercializados, cruzados e utilizados para fins de controle, *marketing* e segurança (Lyon, 2007, p. 45-53; Zuboff, 2019, p. 74-86). A vigilância se converte em infraestrutura invisível das chamadas *smart cities*.

O conceito de cidade inteligente, ou *smart city*, refere-se a um modelo de organização urbana sustentado pela integração entre tecnologias digitais, infraestrutura de dados e formas automatizadas de gestão pública. Conforme Lazzaretti *et al*. (2019), essa noção emerge de uma agenda global de modernização das cidades, em que sensores, câmeras, redes de comunicação e bancos de dados passam a ser utilizados para coletar e processar informações em tempo real, com o objetivo de otimizar serviços e aumentar a eficiência das políticas urbanas.

Nessa perspectiva, a gestão urbana é mediada por plataformas tecnológicas capazes de monitorar fluxos de tráfego, consumo de energia, padrões climáticos, segurança pública e até interações sociais, configurando um ecossistema em que a cidade se torna um grande dispositivo de captação e análise de dados. Ferreira, Novaes e Macedo (2023) destacam que esse modelo implica a criação de uma “infraestrutura de vigilância permanente”, na qual o videomonitoramento e a inteligência artificial são empregados não apenas para fins de segurança, mas também para o controle e a previsão de comportamentos coletivos. A cada movimento de veículos, pedestres e usuários de dispositivos conectados, novos dados são produzidos, armazenados e interpretados por algoritmos de aprendizado de máquina que buscam identificar padrões, antecipar eventos e sugerir intervenções automatizadas. Tal dinâmica confere à cidade um caráter híbrido — simultaneamente físico e informacional — em que o espaço urbano se torna atravessado por sistemas de visibilidade e controle, marcando a consolidação de uma governança algorítmica que redefine a relação entre cidadania, vigilância e poder.

Em termos sociológicos, autores como David Lyon (2007) e Shoshana Zuboff (2019) descrevem as *smart cities* como a forma mais avançada do que chamam de “sociedades de vigilância”. Neste sentido, Lyon (2007) argumenta que a vigilância deixou de ser uma prática excepcional do Estado e tornou-se infraestrutura invisível da vida social, materializada nas redes digitais que registram deslocamentos, hábitos

e interações. Por sua vez, Zuboff (2019), ao desenvolver o conceito de “capitalismo de vigilância”, evidencia que a coleta massiva de dados urbanos não serve apenas à segurança ou eficiência pública, mas também à exploração econômica dos comportamentos humanos, convertendo o cidadão em uma fonte permanente de informação e lucro. Assim, a cidade inteligente emerge como um território de dupla natureza: espaço de inovação tecnológica e, ao mesmo tempo, de intensificação do controle.

O chamado capitalismo de dados designa uma fase do capitalismo em que a extração, circulação e monetização de dados pessoais passam a ocupar o lugar que, em períodos anteriores, foi do petróleo, da terra ou da força de trabalho industrial. Em vez de se limitar a vender bens ou serviços, plataformas digitais e grandes empresas de tecnologia organizam seus modelos de negócio em torno da captura sistemática de rastros informacionais produzidos por usuários, convertendo-os em “matéria-prima” para análise, predição e modulação de comportamentos. Nesse contexto, autores têm falado tanto em capitalismo de vigilância – na formulação de Zuboff (2019) – quanto em capitalismo de dados, para enfatizar que a vigilância deixa de ser apenas um instrumento de segurança estatal e passa a estruturar a própria economia digital, a partir de mercados de predição de conduta e de uma cultura de monitoramento ubíquo e permanente.

Zuboff descreve esse arranjo como uma nova ordem econômica que reivindica unilateralmente a experiência humana como matéria-prima gratuita a ser convertida em dados comportamentais, explorando não apenas aquilo que os sujeitos “dizem” ou “fazem” *online*, mas também inferências sobre o que provavelmente irão desejar, temer ou comprar no futuro (Melo, 2024). Essa lógica, reelaborada em trabalhos recentes brasileiros, aparece como um ecossistema em que a vida cotidiana – gostos, deslocamentos, interações, emoções – é continuamente datificada e minerada, transformando o sujeito em mercadoria e em alvo de uma arquitetura de modificação comportamental. No interior dessa arquitetura, a vigilância deixa de ser apenas um olhar que vigia para punir e converte-se em infraestrutura de extração de valor, em que a assimetria de informação entre plataformas, Estados e usuários é condição para acumulação de dados e poder.

Em artigo, Samuel Cerqueira Melo (2024) retoma a noção de “inteligência de máquina” tal como formulada por Shoshana Zuboff (2019). Neste sentido, Melo (2024) descreve que o capitalismo de vigilância captura a experiência humana como matéria-

prima gratuita, transforma o excedente de dados em “superávit comportamental” e o submete a processos de inteligência de máquina, isto é, a sistemas baseados em *big data*, inteligência artificial e *machine learning* que fabricam produtos de predição capazes de antecipar o que cada indivíduo tende a fazer no presente e no futuro. Ainda em tempo, Melo (2024) destaca que essa capacidade de processamento em velocidade e escala inéditas converte o ser humano em recurso indispensável desse ecossistema de dados, pois é justamente sobre a vida datificada dos usuários que a inteligência de máquina opera e sustenta o poder econômico e político do capitalismo de vigilância.

Pesquisas brasileiras têm mostrado que o capitalismo de dados, tal como se materializa em projetos de cidades inteligentes e em sistemas de reconhecimento facial, opera como uma nova forma de colonialismo voltada ao Sul Global. As infraestruturas digitais e os algoritmos são majoritariamente desenvolvidos por empresas situadas nos países centrais, enquanto países periféricos fornecem, de maneira contínua, os dados que alimentam essas tecnologias. Nesse enquadramento, fala-se em colonialismo de dados para indicar que a promessa de modernização urbana e eficiência na segurança pública convivem com uma dinâmica de extrativismo digital, na qual informações sobre populações periféricas são apropriadas, processadas e monetizadas segundo interesses externos. A datificação da vida cotidiana – mobilidade, consumo, circulação em espaços públicos – tende, assim, a reforçar desigualdades preexistentes de raça, classe, gênero e território, pois os erros e vieses dos sistemas de reconhecimento facial e das redes de videomonitoramento incidem com maior intensidade sobre grupos já historicamente marcados pela suspeita. Esse pano de fundo ajuda a compreender por que a expansão de câmeras “inteligentes” e tecnologias biométricas se concentra em determinados bairros e corpos, transformando cidades brasileiras em verdadeiras colônias de dados dentro da economia global da vigilância (Kronbauer; Oliveira, 2024).

Nesse contexto, os dispositivos de vigilância passam a ocupar posição central no funcionamento do capitalismo de dados. Câmeras de alta resolução, sensores espalhados pela malha urbana, *softwares* de análise automatizada de vídeo e plataformas de gestão de cidades inteligentes formam uma infraestrutura capaz de registrar imagens e movimentos em tempo quase real, alimentando bancos de dados que cruzam localização, biometria, históricos criminais e informações de consumo. Esses arranjos técnicos não apenas “mostram” a cidade, mas qualificam e classificam

aquilo que veem, operando como verdadeiras tecnologias de controle ao mesmo tempo em que são apresentados como soluções de segurança, eficiência e otimização de fluxos urbanos. Com isso, a administração do espaço público passa a ser mediada por sistemas de videomonitoramento que produzem indicadores sobre circulação, permanência, concentração de pessoas e supostas “anormalidades” comportamentais, instaurando novas formas de governo de populações e territórios baseadas na extração e no tratamento intensivo de dados (Bordignon, 2020).

As chamadas “câmeras inteligentes” exemplificam a passagem de um modelo de vigilância centrado apenas no registro visual para um regime em que ver já implica classificar, analisar e decidir. Em vez de somente transmitir imagens a uma sala de controle, esses dispositivos são acoplados a algoritmos capazes de reconhecer padrões, identificar rostos e placas, medir fluxos e detectar automaticamente situações definidas como “suspeitas” em espaços como ruas, praças, estádios ou estações de transporte, operando de forma distribuída no tecido urbano, essas câmeras atuam no próprio fluxo da vida cotidiana, sem necessariamente produzir intervenções visíveis nos deslocamentos dos corpos, mas convertendo continuamente gestos, trajetórias e aglomerações em sinais que alimentam sistemas automatizados de alerta e classificação de risco (Bruno, 2012). Do ponto de vista econômico, essa capacidade de transformar movimentos em dados categorizados torna-se valiosa tanto para órgãos públicos quanto para empresas privadas, que podem adquirir serviços de predição, mapeamento de “pontos quentes” de criminalidade ou análise de circulação urbana, reforçando a articulação entre segurança, gestão da cidade e mercados de dados.

Ao tratar da subjetivação contemporânea em meio às tecnologias digitais, Pablo Esteban Rodriguez (2015) mostra que a vigilância hoje se articula diretamente a novos modos de ser sujeito, redefinindo os limites entre o público, o privado e o íntimo. Partindo de autores como Foucault, Deleuze e Debord, ele argumenta que, nas redes sociais, práticas de exposição de si e de gestão de perfis se entrelaçam a lógicas de controle, de modo que o indivíduo passa a ser pensado como “dividual”, um conjunto de fragmentos, rastros e dados permanentemente observáveis e recombináveis. Nesse cenário, a sensação de estar potencialmente visível o tempo todo – para outros usuários e para sistemas automatizados – passa a compor a experiência de si, produzindo subjetividades atravessadas por métricas, avaliações e formas distribuídas de vigilância que se tornam imanentes ao próprio cotidiano.

Os algoritmos das plataformas digitais vêm sendo descritos como dispositivos que organizam a visibilidade e, ao fazê-lo, modelam formas de sociabilidade e de relação consigo mesmo. Em vez de operarem como filtros neutros, eles selecionam, ranqueiam e recomendam conteúdos a partir de critérios de relevância que articulam interesses comerciais, lógicas de engajamento e formas específicas de participação. Esse funcionamento, baseado em coleta contínua de dados, construção de perfis e retroalimentação dos fluxos informacionais, produz ambientes marcados por métricas, índices de desempenho e hierarquias de atenção que favorecem câmaras de eco e reduzem o espaço para a diferença. A subjetividade que se constitui nesse contexto passa a ser atravessada por notificações, contagens de visualizações e parâmetros algorítmicos opacos, de modo que o “eu” se vê convocado a gerir-se permanentemente como um projeto de otimização e visibilidade, conforme analisado em estudos brasileiros sobre subjetividade e vigilância nas redes sociais digitais (Ferreira, 2025).

A literatura sobre capitalismo de vigilância e constituição do sujeito mostra que a coleta e a mineração de dados digitais operam como mecanismos de poder que atravessam diretamente a experiência subjetiva. Ao converter ações cotidianas em dados e, depois, em perfis e previsões, esses sistemas produzem uma “anatomia política do eu”, na qual desejos, opiniões, hábitos de consumo e posicionamentos políticos são continuamente monitorados e modulados. O sujeito contemporâneo é, ao mesmo tempo, usuário, consumidor e recurso, sua presença em plataformas digitais implica estar permanentemente vigiado, classificado e suscetível a intervenções comportamentais nem sempre visíveis, que vão da personalização de anúncios e notícias ao ranqueamento de candidatos a emprego, à concessão de crédito e à definição de prioridades em políticas de segurança (Melo, 2024).

Quando essas lógicas de vigilância algorítmica se acoplam a infraestruturas de segurança pública – como redes de videomonitoramento, centrais de comando e controle e sistemas de reconhecimento facial – os processos de subjetivação ganham dimensão ainda mais sensível. Análises sobre tecnologias inteligentes de vigilância indicam que tais arranjos funcionam como mecanismos de governamentalidade afinados a racionalidades neoliberais (Ribeiro, 2018), prometendo segurança sem interromper fluxos e deslocando a disciplina direta sobre corpos para o controle ambiental por meio da análise contínua de dados e padrões. Em cidades marcadas por desigualdades profundas, isso faz com que determinados grupos e territórios se

tornem alvos recorrentes de suspeita e monitoramento, enquanto outros vivenciam sobretudo a sensação de proteção, naturalizando a expansão de câmeras e algoritmos como preço a pagar pela segurança. Nessa ambiência, sujeitos são interpelados ora como consumidores de serviços securitários, ora como potenciais ameaças, ora como conjuntos de dados que circulam em ecossistemas digitais.

3.4 CÁRCERE, DISTÂNCIA SOCIAL E PRODUÇÃO DE VERDADE: PONTE PARA A VIGILÂNCIA ALGORÍTMICA

A proposta desta seção é tratar o cárcere como um caso-limite que torna visíveis mecanismos sociais de classificação, hierarquização e legitimação do controle, permitindo compreender como tais mecanismos são reconfigurados e escalados por infraestruturas digitais e sistemas de inteligência artificial. Em vez de opor “prisão” e “tecnologia” como temas distintos, a análise toma o cárcere como ponte, ou seja, aquilo que a prisão concentra em muros e rotinas institucionais tende a reaparecer, em chave distribuída na vigilância algorítmica que opera por dados, probabilidades e correlações (Toscano, 2012, p. 83).

Segundo o livro organizado ‘Cárcere e Cidade’, a materialidade do cárcere produz um efeito de evidência por parecer “concreto” e autoexplicativo, ele favorece a impressão de que seria desnecessário explicar o que é uma penitenciária, como se o espaço “falasse por si” (Toscano, 2012, p. 83). Esse mesmo efeito epistemológico se repete na governança algorítmica, na qual *dashboards*, métricas e *outputs* de modelos (alertas, *scores*, correspondências biométricas) muitas vezes são recebidos como fatos “objetivos”, encobrindo o conjunto de escolhas normativas que definem o que será medido, quais categorias serão usadas e quais resultados serão considerados relevantes. Assim, tanto no cárcere quanto na IA, a crítica precisa deslocar o olhar do “objeto” (muro ou algoritmo) para os procedimentos que produzem visibilidade, suspeição e decisão.

Outro ponto decisivo é que o cárcere não opera como universo isolado. A análise enfatiza a porosidade das prisões e sua inserção em relações que não se originam apenas no interior da instituição, mas que também são constitutivas de vínculos com o “fora”. Essa porosidade ajuda a compreender por que a vigilância algorítmica não deve ser tratada apenas como ferramenta “da polícia” ou “do Estado”, mas, como ecossistema sociotécnico que atravessa cidades, serviços e rotinas

administrativas como dados urbanos, videomonitoramento e integrações de sistemas que fazem com que lógicas historicamente associadas ao penal se projetem sobre o cotidiano, modulando circulação, abordagens e prioridades de intervenção (Toscano, 2012, p. 84).

Ao tratar dos valores e da demarcação das distâncias, o capítulo ‘Notícias da Cloaca Máxima’, inserido na coletânea ‘Cárcere e Cidade’, desloca a discussão do crime como essência para o crime como processo social de atribuição de sentido, valoração e hierarquização, no qual a produção do “desvio” se vincula a separações simbólicas e materiais entre grupos (Toscano, 2012, p. 85-86). O ganho dessa chave para a inteligência artificial é direto, sistemas de classificação automatizada tendem a converter desigualdades prévias — território, raça, classe e históricos seletivos de abordagem — em “sinais” de risco, reproduzindo distâncias sociais sob a forma de triagens técnicas e decisões probabilísticas. Essa interpretação dialoga com a tradição dos estudos de vigilância que descrevem a vigilância digital como *social sorting*, isto é, uma ordenação social por critérios de risco, perfil e acesso, na qual a administração de populações se realiza por categorias operacionais e classificações contínuas, e não apenas por coerção explícita.

Nesse enquadramento, a noção de desvio é “desessencializada”, pois rejeita-se a passagem do ato à pessoa como falácia que transforma condutas em identidades e naturaliza a existência de sujeitos “inerentemente desviantes” (Becker, 2008; Toscano, 2012, p. 93). Quando transposta para a vigilância algorítmica, essa crítica ilumina um risco central, os perfis probabilísticos (“alto risco”, “suspeito”, “propenso”) podem funcionar como identidades técnicas que aderem ao indivíduo, reforçando estigmas e ampliando assimetrias na ação estatal. O problema não se limita ao erro estatístico, trata-se da produção de um rótulo que circula com autoridade institucional e pode orientar intervenções cumulativas. Em termos sociotécnicos, configura-se um *feedback loop*. A intensificação do monitoramento gera mais dados sobre os mesmos alvos e, esses dados tendem a calibrar o sistema para reproduzir as mesmas prioridades de vigilância, reforçando a aparente “evidência” que sustenta o próprio modelo.

A conexão entre cárcere e IA torna-se ainda mais nítida quando se introduz a questão da produção de verdade. Ao invés de tratar “verdade” como unidade pacífica, a análise aponta disputas e procedimentos de validação que vinculam verdade, poder e direito. Em ambientes algorítmicos, essa articulação se traduz na transformação de

outputs técnicos em “verdades operacionais”, ou seja, um *match* biométrico, um *score* ou um alerta pode ser suficiente para justificar abordagem, encaminhamento, retenção ou investigação, e depois ser reafirmado por rotinas administrativas e discursos jurídicos. O foco crítico, portanto, não é apenas “vigiar”, mas compreender como se produz e se legitima uma verdade tecnicamente mediada que impacta direitos e liberdades.

No Brasil, a literatura recente sobre reconhecimento facial e videomonitoramento mostra como essa “verdade operacional” pode se consolidar em políticas públicas antes mesmo de existirem salvaguardas robustas de auditabilidade e contestação. Estudos têm discutido parâmetros mínimos de legitimidade, riscos de discriminação e a necessidade de limites jurídicos ao uso de reconhecimento facial automatizado em tempo real na persecução penal (Almeida, 2022). Também em nível de pós-graduação, pesquisas analisam o reconhecimento facial como forma de vigilância de massa e destacam tensões éticas e jurídicas relacionadas a direitos humanos, devido processo e segregação/discriminação (Duarte; Oliveira, 2025). Esses trabalhos reforçam que a “ponte” com o cárcere não é metáfora solta, trata-se de entender como a racionalidade punitiva se reconfigura quando passa a operar por biometria, bancos de dados e inferências.

Desse modo, a ponte entre cárcere e vigilância algorítmica se fecha no plano normativo e metodológico. Se o poder circula por redes técnicas e se a verdade é produzida por procedimentos, então a regulação não pode se limitar a autorizar “uso de IA” em abstrato, devendo incidir sobre dados, critérios, finalidades e responsabilização.

4 VIDEOMONITORAMENTO INTELIGENTE EM PERNAMBUCO COM IDENTIFICAÇÃO DE PLACAS DE VEÍCULOS

4.1 ESTRUTURA E EXPANSÃO DO SISTEMA DE CÂMERAS EM PERNAMBUCO

Nos últimos anos, o Estado de Pernambuco tem promovido uma acelerada modernização de sua estrutura de segurança pública, na qual o videomonitoramento inteligente figura como componente estratégico central. Notadamente, a identificação automática de placas de veículos (LPR/ALPR) surge como tecnologia-chave para rastrear fluxos veiculares, apoiar investigações criminais e articular as áreas de trânsito, logística e segurança. Esse movimento não se dá apenas como adição de câmeras, mas como implantação de um ecossistema de imagem-dados que combina câmeras digitais de alta resolução, algoritmos de leitura automática de caracteres, bancos integrados de veículos e centros de comando em tempo real.

Do ponto de vista metodológico, este capítulo descreve a estrutura técnico-institucional do sistema (centros de gerenciamento, enlaces de comunicação, distribuição territorial e licenças analíticas) e, em seguida, discute como a IA é incorporada às rotinas investigativas e de gestão de ocorrências. A intenção é explicitar a “cadeia sociotécnica” que vai da câmera ao procedimento, no qual se decide o que é captado, como é classificado, por quais parâmetros se produz um alerta e de que modo esse alerta se converte em solicitação de imagem, relatório, diligência e eventual prova.

Do ponto de vista institucional, a ampliação do videomonitoramento em Pernambuco se articula com programas estaduais como o “Juntos pela Segurança”, que firmou contrato relevante para instalação de 2 mil câmeras em municípios da Região Metropolitana do Recife e de cidades do interior, com leitura de placas veiculares e integração aos centros de gerenciamento da Secretaria de Defesa Social (SDS) (sds.pe.gov.br, 2024). A expansão contempla tanto equipamentos fixos em ruas e avenidas quanto soluções móveis, ligadas ao controle de trânsito e fiscalização veicular, o que evidencia a convergência entre segurança pública, mobilidade urbana e tecnologia de dados. Ademais, municípios como Recife, Cabo de Santo Agostinho e Afogados da Ingazeira já operam suas próprias redes ou soluções complementares, criando um panorama de múltiplas instâncias – estadual, municipal e operacional – de videomonitoramento.

Tecnicamente, a identificação automática de placas envolve uma cadeia que começa com a captação da imagem da placa por câmera de alta resolução, segue com o processamento por algoritmo de reconhecimento óptico de caracteres (OCR), conexão com banco de dados para verificação da situação do veículo (roubo, furto, impedimentos administrativos) e geração de alerta em tempo real. Essa cadeia permite antecipar ações como abordagem, bloqueio ou recuperação de veículos, mas também requer bases de dados confiáveis, infraestrutura de rede estável e protocolos de segurança da informação. Além disso, a leitura de placas integrada a vídeo inteligente abre espaço para cruzamentos com fluxos de pessoas, logística de cargas e padrões de deslocamento, transformando o sistema em instrumento investigativo e de inteligência urbana.

Essa transformação técnica insere-se em um contexto mais amplo de cidades inteligentes e de vigilância algorítmica, em que a infraestrutura física do monitoramento se articula a redes de comunicação, bases de dados e rotinas automatizadas de processamento. Segundo Lazzaretti *et al.* (2019, e20180018), essa integração tecnológica permite “[...] a coleta e análise de dados em tempo real para gerenciar recursos de maneira eficaz, facilitando [...] a segurança pública”. Nessa lógica, cada veículo capturado pela câmera converte-se em dado potencialmente analisável, e o deslocamento urbano passa a produzir indicadores úteis à prevenção e à investigação. No caso pernambucano, a adesão a essas tecnologias expressa não apenas a busca por melhores resultados na segurança, mas também o aproveitamento de financiamentos, parcerias e incentivos vinculados à modernização da gestão pública.

A contratação pública recente descreve o videomonitoramento como “solução integrada” voltada não só à captação e visualização, mas também ao processamento, análise e gestão de eventos, com operação técnica especializada e adaptação física dos centros de comando (Pernambuco, 2024). Essa caracterização é relevante porque indica uma mudança de regime. O sistema passa a ser pensado como serviço contínuo de infraestrutura (e não como conjunto de equipamentos), com requisitos de conectividade, redundância e sustentação que condicionam a própria disponibilidade das imagens.

No desenho técnico do parque, a expansão se expressa tanto na quantidade de pontos de captura quanto na diversificação dos tipos de câmera. O Termo de Referência prevê 1.347 pontos de captura de imagem (*PCI*), distribuídos entre

câmeras fixas, câmeras *PTZ* e câmeras panorâmicas, incluindo 378 câmeras com *LPR* capazes de leitura em condições de deslocamento rápido (até 200 km/h, conforme especificação) (Pernambuco, 2024). Em termos analíticos, isso significa que a identificação veicular não é “um módulo à parte”, mas um componente integrado ao parque, com implicações diretas para a priorização de vias, corredores e zonas de interesse operacional.

A arquitetura institucional do monitoramento se organiza por centros de gerenciamento. Há um Centro de Gerenciamento Central (CGC) no CIODS, no Recife, e dois Centros de Gerenciamento Independentes (CGI) em cidades do interior — um em Caruaru e outro em Petrolina — com estimativas de PCI gerenciados por unidade (701 no CGC, 411 no CGI Caruaru e 235 no CGI Petrolina) (Pernambuco, 2024). Essa distribuição territorial indica uma estratégia de capilaridade com governança centralizada. O monitoramento não depende apenas da instalação de câmeras, mas da capacidade de ingestão e gerenciamento de fluxos (*links*, gravação, busca e recuperação) em rotinas 24/7.

Nesse ponto, a conectividade se torna parte constitutiva do “funcionar” do sistema. O projeto prevê enlace por fibra óptica entre o CGC e a sala cofre da ATI, com redundância de rotas e equipamentos, para reduzir dependências de enlaces externos e mitigar interrupções por falhas físicas (Pernambuco, 2014). A consequência é simples e decisiva. A promessa de “inteligência” depende da estabilidade do *pipeline* de dados, sem tráfego sustentado de vídeo e metadados, *LPR*, busca forense e alertas se degradam em desempenho e confiabilidade.

No plano econômico-administrativo, a expansão também se evidencia na discrepância entre os quantitativos e valores apresentados nos documentos licitatórios e aqueles divulgados em comunicação institucional e cobertura jornalística. O edital prevê contratação por 60 meses e inclui, no escopo, licenças analíticas (como *VMS* e *LPR*) e demais componentes da solução integrada. Em paralelo, registros públicos indicam a implantação de 2 mil câmeras com uso de IA e investimento de R$ 122,9 milhões, com ênfase na Região Metropolitana e em municípios estratégicos do interior. A diferença entre 1.347 pontos de captura de imagem (*PCI*) projetados no Termo de Referência e as 2 mil câmeras mencionadas em anúncios públicos (sds.pe.gov.br, 2024) sugere a existência de fases e/ou escopos distintos, bem como possíveis diferenças conceituais entre *PCI* e “câmeras instaladas/ativas”, recomendando

cautela na comparação entre capacidade projetada e capacidade efetivamente operacional.

4.2 UTILIZAÇÃO DOS MECANISMOS DE VIGILÂNCIA PELA POLÍCIA

O *License Plate Recognition* (*LPR*), também referido como *Automatic Number Plate Recognition* (*ANPR*), é uma tecnologia de visão computacional que automatiza a identificação de veículos ao converter a imagem da placa em um dado textual estruturado. De modo geral, o processamento envolve a detecção da região da placa no quadro, etapas de tratamento de imagem para lidar com ruído, distorções e variações de iluminação, e o reconhecimento óptico de caracteres (*OCR*) para extrair a sequência alfanumérica (Mufti; Muhammad; Hussain, 2021). O produto final não é apenas “imagem”, mas um registro pesquisável que pode ser comparado com listas e bases, permitindo que a circulação veicular seja tratada como evento e não apenas como fluxo visual contínuo (Tang *et al*., 2022).

No desenho do videomonitoramento em Pernambuco, a unidade usada para dimensionar a implantação é o PCI (Ponto de Captura de Imagem). Trata-se do “ponto” operacional de captação no território (o local de instalação/monitoramento), que pode corresponder a uma câmera única ou a um arranjo de câmeras e acessórios, conforme a finalidade do ponto (Pernambuco, 2024). Essa distinção é relevante porque o planejamento do sistema nem sempre se expressa em “número de câmeras”, mas em “pontos de captura”, o que afeta comparações entre capacidade projetada e capacidade instalada, sobretudo quando diferentes tipos de pontos exigem composições distintas de equipamentos e infraestrutura.

Ainda no âmbito do *LPR*, o Termo de Referência divulgado no processo licitatório de Pernambuco prevê PCIs específicos destinados à leitura de placas em vias e condições de deslocamento elevado, incluindo especificação de leitura em veículos em alta velocidade e, em alguns casos, a combinação de câmera fixa e câmera dedicada ao *LPR* no mesmo ponto (Pernambuco, 2024). Essa configuração indica que a identificação veicular é concebida como eixo estruturante do parque. O objetivo não é apenas gravar imagens, mas capturar evidências indexáveis de circulação, aptas a alimentar alertas, buscas retrospectivas e cruzamentos com listas de interesse.

A gestão dos fluxos de videomonitoramento e a operacionalização dos analíticos dependem, em regra, de um *VMS* (*Video Management System*), entendido como um sistema de gerenciamento de vídeo responsável por reunir, em uma mesma camada, a administração dos fluxos provenientes das câmeras e a organização do acervo de gravações. Nesse sentido, o *VMS* funciona como a “espinha dorsal” do videomonitoramento digital, estruturando como as imagens são recebidas, registradas e disponibilizadas para consulta e operação (GENETEC, [s.d.]).

Em termos operacionais, o *VMS* centraliza atividades como visualização em tempo real, gravação, reprodução e busca no histórico, oferecendo mecanismos de pesquisa e recuperação de material conforme parâmetros definidos pela instituição (por exemplo, período, câmera, evento e outros filtros) (Silva; Silva; Lorenção; Barros, 2020). Além disso, ao organizar o acesso ao acervo e as telas de monitoramento, o sistema tende a padronizar rotinas de trabalho e a reduzir a dependência de inspeção manual contínua, pois permite navegar por ocorrências e localizar trechos relevantes com maior rapidez.

Essa camada é decisiva para que o *LPR* deixe de ser um processamento isolado e passe a integrar um ecossistema de decisão em tempo quase real. Ao incorporar eventos e metadados gerados por analíticos (como leituras de placa e alertas associados), o *VMS* transforma o vídeo em informação operacional. Em vez de apenas “assistir” às imagens, o operador passa a consultar registros, aplicar filtros e recuperar evidências vinculadas a ocorrências (A3A Engenharia, [s.d.]). Assim, a efetividade do *LPR* depende não só do reconhecimento em si, mas também da capacidade do *VMS* de indexar, relacionar e disponibilizar esses resultados de forma rastreável e útil ao trabalho investigativo.

Assim, do ponto de vista investigativo, o *LPR* adquire valor por transformar a leitura em banco de dados, uma vez que as especificações incluem armazenamento das placas reconhecidas associadas a foto e marca temporal (data e horário), além de listas e busca forense por atributos como cor, padrão de placa e placa parcial. Também se prevê o registro de variáveis e características do veículo (por exemplo, pista, placa, velocidade estimada, cor, marca e tipo/categoria), ampliando a capacidade de reconstrução retrospectiva de trajetórias e geração de alertas operacionais.

Deste modo, a incorporação da IA ocorre, primeiramente, pela passagem do vídeo entendido como imagem contínua para o vídeo tratado como conjunto de

eventos indexáveis. Em termos operacionais, isso significa que o sistema deixa de depender apenas da assistência humana a longas gravações e passa a gerar “marcas” no fluxo (eventos) a partir de analíticos — por exemplo, leitura de placas (*LPR*), detecção de aglomeração e mecanismos de busca forense —, permitindo localizar trechos relevantes por filtros e critérios previamente definidos, em vez de revisar o material integralmente (Pernambuco, 2024).

Essa mudança reorganiza o tempo do trabalho policial e investigativo. Parte do esforço que antes era triagem manual é deslocada para a filtragem automatizada, que prioriza ocorrências a partir de regras de detecção e parâmetros de configuração do próprio sistema. Esses parâmetros incluem limiares (pontos de corte) que determinam quando um comportamento/condição será registrado como evento ou alerta. No caso do analítico de detecção de aglomeração, por exemplo, o documento técnico prevê o reconhecimento de um “número específico” ou “predeterminado” de pessoas em uma área e a geração de alertas quando esse limite é excedido, isto é, quando o limiar configurado é ultrapassado.

Em linguagem de sistemas de classificação, “limiar” é o ponto de corte usado para mapear um resultado contínuo (ou uma medida de confiança) em uma decisão binária (alertar/não alertar; aceitar/rejeitar), o que ajuda a compreender por que a eficácia prática depende tanto da calibragem desses pontos de corte quanto do próprio modelo (Batistella, 2025). Além disso, ao prever que a busca forense gere eventos ao identificar padrões pré-estabelecidos ou similaridades de características (para pessoas e veículos), o edital de licitação indica que a investigação passa a operar com um repertório de filtros e métricas (cor, acessórios etc.) que tornam o acervo pesquisável e “navegável” por critérios analíticos, reduzindo o tempo de localização de evidências.

Nesse cenário em que a análise automatizada transforma o acervo em algo “pesquisável” por critérios (limiares, filtros e padrões), o *LPR* se apresenta como um caso particularmente elucidativo. Trata-se de um analítico que não apenas “observa” o trânsito, mas produz registro formal de passagem veicular, apto a ser consultado, cruzado e acionado em rotinas operacionais. Em outras palavras, o valor investigativo do *LPR* decorre de deslocar o vídeo do regime da mera visualização para o regime do dado indexado, no qual cada leitura passa a existir como ocorrência catalogada pelo sistema, com campos específicos que permitem rastreabilidade e consulta posterior.

O salto técnico-jurídico do *LPR* começa na conversão da imagem em dado estruturado. A câmera registra o veículo, o sistema localiza a placa e, por meio de reconhecimento de caracteres, transforma a sequência alfanumérica em texto, associando essa leitura a elementos contextuais como data, hora e local. Esse processo é relevante para o Direito porque altera o estatuto da informação. O que antes era “imagem a interpretar” passa a ser também “registro a consultar”, com potencial de orientar diligências e hipóteses investigativas a partir de rastros de mobilidade. Em revisões recentes sobre reconhecimento automático de placas, a tecnologia é descrita justamente como meio de registrar movimentos veiculares e produzir informação manipulável em bancos de dados, o que explica sua centralidade em políticas de mobilidade e segurança (Tang *et al*., 2022).

No modelo previsto para Pernambuco, essa estruturação aparece de forma explícita nas exigências de registro. O sistema deve armazenar placas reconhecidas com imagem associada (foto), marca temporal (data e horário) e elementos de localização, além de admitir buscas e cruzamentos por atributos úteis para a prática policial, como cor do veículo e placa parcial (Pernambuco, 2024). Para uma leitura jurídica, importa notar que não se está diante de simples gravação, pois o que se projeta é uma base consultável que permite localizar eventos por critérios objetivos (tempo, lugar e características), facilitando reconstruções retrospectivas (“por onde passou”, “em que horário”, “em qual ponto de captura”) e instruções de busca orientadas por parâmetros definidos.

Esse desenho tem implicações probatórias e procedimentais importantes, pois desloca o “centro de gravidade” do vídeo para os metadados produzidos pela ferramenta. Na prática cotidiana, o achado investigativo tende a aparecer primeiro como ocorrência sinalizada (um alerta de passagem, uma correspondência com lista de interesse, um registro recuperado por busca), e só depois é “reancorado” na gravação original que o sustenta. Isso exige atenção metodológica, visto que para que a informação seja confiável em termos de prova, torna-se fundamental garantir a possibilidade de verificação posterior (revisão do trecho, preservação do arquivo e coerência entre registro e imagem), especialmente porque literatura técnica aponta que desempenho e erros podem variar conforme velocidade (Cordeiro, 2015), ângulo, iluminação e condições do ambiente — fatores que podem produzir leituras equivocadas se não houver protocolos de validação.

Quando o *LPR* é integrado ao fluxo de trabalho, a tendência é haver ganhos de coordenação operacional, porquanto o sistema pode apoiar desde a gestão de ocorrências urbanas até solicitações investigativas, fornecendo recortes temporais e eventos de interesse para instrução de procedimentos.

No caso Pernambucano, a própria comunicação pública sobre a implantação tem associado o videomonitoramento a resultados operacionais e a suporte a ações de polícia, o que sugere que a tecnologia não fica restrita à sala de controle, mas se articula com despacho, patrulhamento e investigação (Diário de Pernambuco, 2025). Para o Direito, esse ponto é relevante porque evidencia uma mudança de rotina, dado que o videomonitoramento deixa de ser "mera fonte de imagem" e passa a integrar o circuito de decisão, com efeitos sobre tempo de resposta, geração de relatórios e priorização de diligências.

4.3 LPR E GOVERNAMENTALIDADE ALGORÍTMICA DA CIRCULAÇÃO

O que o LPR introduz no videomonitoramento não é apenas uma melhoria do "ver", mas uma mudança no estatuto da circulação como objeto de governo. Quando a passagem de um veículo é convertida em um registro estruturado (placa + tempo + local + imagem associada), a circulação deixa de ser um acontecimento que desaparece no instante seguinte e passa a funcionar como rastro arquivável, recuperável e combinável com outros rastros. No regime tradicional da vigilância por imagem, buscava-se muitas vezes "a cena" (o episódio pontual) e dependia-se de revisão posterior; com o LPR, ganha centralidade a regularidade, porque é a recorrência que se torna comparável, pesquisável e acionável ao longo do tempo (Cordeiro, 2015).

Esse deslocamento é técnico e, ao mesmo tempo, epistemológico. A imagem deixa de valer somente como imagem e passa a valer como entrada de um processo que extrai caracteres, associa tempo e lugar, produz metadados e entrega uma ocorrência pronta para consulta dentro de um ecossistema de gestão. No caso pernambucano, o próprio Termo de Referência descreve a contratação como "solução integrada" que não se limita à visualização, mas envolve processamento, gestão de eventos e mecanismos operacionais de acesso, registro e auditoria, o que torna plausível ler o videomonitoramento como um ambiente informacional e não apenas como um conjunto de câmeras (Pernambuco, 2024). Nesse quadro, a vigilância se

desloca do “contemplar” para o “operar”, ou seja, localizar, filtrar, cruzar, recuperar e registrar.

É nesse sentido que a noção de governamentalidade algorítmica ajuda a dar precisão ao capítulo. Em Rouvroy e Berns, a governamentalidade algorítmica não se define por mandar ou proibir diretamente, mas por conduzir o campo do possível por meio de estatísticas, correlações e antecipações, produzindo prioridades e seleções a partir de dados (Rouvroy; Berns, 2015). O que importa nessa racionalidade não é explicar o sujeito por sua interioridade, mas tratá-lo como ponto de passagem por padrões, de modo que o governo se faz pela gestão de relações entre medidas. Quando um sistema de LPR transforma a mobilidade em banco consultável e produz alertas por listas e critérios de correspondência, ele se encaixa nesse regime, ele governa menos por ordem explícita e mais por seleção automática do que merece atenção.

Essa leitura não elimina o Panoptismo; ela o desloca. Em Foucault, o Panoptismo é um diagrama de poder centrado na assimetria de visibilidade e na produção de condutas pelo fato de poder ser visto. No LPR, porém, a visibilidade se traduz em unidades manipuláveis: texto, tempo, coordenada, lista e alerta. A vigilância se torna uma forma de escrita sobre o movimento, na qual o poder opera menos como o olhar que intimida no presente e mais como arquivo que pode ser reativado a qualquer momento. Essa reativação muda o tempo do controle. O que antes precisava de presença constante (o vigia atento) passa a depender do potencial de recuperação, não sendo necessário acompanhar tudo agora se o rastro pode ser buscado depois (Foucault, 2014, p. 190-194). O presente “engrossa” porque cada passagem pode virar retrospecto, cada trajeto pode virar sequência e cada coincidência pode ser reconstruída como narrativa posterior. Essa é uma característica importante do LPR, ele não precisa ser total para produzir efeitos, basta ser suficientemente indexável, isto é, capaz de gerar rastros com consistência e de conectá-los a critérios de busca.

O VMS, nesse arranjo, funciona como o operador dessa virada do olhar para a consulta. Em vez de “assistir” ao fluxo contínuo, o operador navega por eventos, filtros e recortes, e a cidade aparece em janelas de relevância. No Termo de Referência de Pernambuco (Pernambuco, 2014), a ênfase na integração e na gestão da plataforma — inclusive com rastreabilidade por *logs* e trilhas de auditoria — aponta para uma operação que é menos cinematográfica (acompanhar tudo) e mais informacional (buscar aquilo que o sistema marcou como relevante).

Nesse regime, “padrão” não é uma constatação neutra, é um operador político-técnico. Deste modo, “padrões” são aquilo que o sistema aprende a reconhecer, e reconhecer implica reduzir, converter a complexidade do real em traços comparáveis. Fernanda Bruno (2012, 2013, 2018) enfatiza que rastrear e classificar não apenas descrevem o mundo, eles o performam, porque as categorias de captura e indexação definem o que conta como dado e o que passa a importar. Assim, quando o LPR organiza o acervo por critérios e o torna consultável, ele também define quais movimentos entram na gramática do controle e quais permanecem invisíveis como “não-evento”.

A suspeição, então, pode emergir como efeito de arquitetura e não apenas como intenção subjetiva. Ela não precisa começar no “desconfiei”, pode começar no “o sistema apontou”, quando listas, limiares e cruzamentos fazem aparecer uma correspondência como alerta. Essa forma operacional do alerta tende a carregar uma aparência de objetividade, porque vem empacotada como saída técnica, e isso reorienta o modo como decisões são justificadas no cotidiano do policiamento (Bruno, 2016).

É aqui que a noção de “social *sorting*” se torna útil. David Lyon (2003) descreve a vigilância contemporânea como ordenação social por categorias de risco e perfis, na medida em que bancos pesquisáveis permitem classificar, atribuir valor, selecionar e distribuir atenção de forma desigual. No LPR, embora o alvo imediato seja o veículo, o efeito social pode ser a produção de diferentes graus de legibilidade para rotas, horários e territórios. O que é mais indexável aparece mais, o que é menos indexável desaparece. O controle passa a incidir não apenas sobre desvios, mas sobre o que pode ser construído como evento relevante. Essa ordenação é espacial.

Firmino (2017) propõe pensar tecnologias de vigilância como camadas territoriais que se sobrepõem à cidade, criando zonas mais monitoradas, corredores mais legíveis e áreas de maior acionamento. Quando a circulação vira dado, o território vira também um mapa de probabilidades e prioridades, e a cidade deixa de ser apenas cenário para se tornar infraestrutura de governo. No caso pernambucano, a distribuição do sistema por centros de gerenciamento e pontos de captura reforça que a governança do olhar é, ao mesmo tempo, tecnológica e territorial.

A aproximação com Deleuze (2013) ajuda a dar nome ao tipo de poder que se desenha nessa modulação contínua. Na “sociedade de controle”, o poder opera por

ajustes e filtros, não apenas por recintos fechados; ele modula fluxos em vez de apenas disciplinar corpos em instituições.

O *LPR* combina com essa lógica porque não precisa impedir a circulação, ele mede, cruza e prioriza a circulação, transformando deslocamentos em variável governável, com decisões distribuídas por parâmetros, listas e limiares.

Essa modulação é muitas vezes silenciosa, porque se faz por microdecisões de relevância, em outras palavras, qual lista terá prioridade? Qual correspondência disparará? Qual zona será monitorada com mais intensidade? Parâmetros condensam escolhas sobre tolerância, risco e erro aceitável, e essas escolhas retornam ao social como efeitos concretos de atenção e intervenção. Esse ponto dialoga com o alerta de Edson Teles sobre subjetivações rarefeitas, pois quando a racionalidade de governo se organiza por cálculo e previsão automatizada, o sujeito tende a aparecer mais como variável do que como interlocutor, e o conflito sobre fins pode ser substituído por gestão de meios (Teles, 2018).

Por fim, é preciso reconhecer que a governamentalidade algorítmica depende de um ambiente técnico atravessado por incerteza. Trabalhos técnicos e acadêmicos sobre reconhecimento de placas registram variações de desempenho conforme ângulo, iluminação, velocidade e oclusão, o que significa que o “padrão” é sempre inferido sob ruído e que a calibragem dos limiares é parte do governo por dados (Bernardi, 2016). Quando a decisão se apoia em arquivo e índice, a confiabilidade da infraestrutura deixa de ser detalhe, ela vira condição de possibilidade do próprio regime de prova e de decisão.

5 FORMAS DE POLICIAMENTO E A CONSTRUÇÃO DO BOM POLICIAMENTO

A reflexão sobre o que caracteriza o bom policiamento passa necessariamente pela compreensão de que a atividade policial não é homogênea nem estática. Ao longo do tempo, diferentes formas de organização e atuação policial foram desenvolvidas em resposta a transformações sociais, políticas e institucionais. Esses modelos não representam apenas variações técnicas ou administrativas, mas expressam distintas concepções sobre o papel da polícia, sobre os limites do poder estatal e sobre a própria ideia de segurança pública em sociedades democráticas.

Entre as formas mais influentes de organização policial encontra-se o chamado policiamento profissional. Consolidado sobretudo ao longo do século XX, esse modelo procurou estruturar a atividade policial a partir de critérios de racionalização burocrática, especialização funcional e padronização de procedimentos. A disciplina organizacional, a formação técnica e a separação entre polícia e política passaram a ser vistas como elementos capazes de conferir maior previsibilidade à atuação policial e de reduzir a arbitrariedade decorrente de improvisação ou interferência direta de interesses locais imediatos (Bayley, 2002, p. 35, 50, 60).

Essa forma de policiamento pode ser compreendida com maior precisão a partir da análise de David H. Bayley (2002) sobre o desenvolvimento da polícia moderna. Ao examinar comparativamente a evolução do policiamento, o autor sustenta que a polícia contemporânea é marcada por três atributos principais: seu caráter público, sua condição especializada e sua feição profissional. Esses três traços não aparecem em Bayley como uma definição abstrata ou atemporal da polícia, mas como a combinação histórica que passou a predominar no mundo moderno.

O primeiro atributo é o caráter público da polícia, pois, para o escritor, a polícia só se torna efetivamente pública quando é, ao mesmo tempo, paga e controlada pela coletividade (Bayley, 2002) Isso significa que o simples fato de a polícia estar ligada ao governo não basta, por si só para qualificá-la como pública em sentido pleno. O ponto central está em que tanto o financiamento quanto a direção da atividade policial sejam exercidos em nome da comunidade política. Há, portanto, nesse atributo, uma dimensão institucional e uma dimensão normativa, digo, a polícia pública não é apenas estatal, mas vinculada à ideia de atuação em nome do interesse coletivo.

Em termos mais simples, Bayley (2002) mostra que a polícia não é verdadeiramente “pública” apenas porque pertence ao Estado ou porque integra a

estrutura do governo. Para que ela seja pública em sentido pleno, é necessário que sua manutenção e sua orientação ocorram em nome da coletividade, isto é, que ela seja sustentada com recursos públicos e dirigida para atender a interesses públicos. Isso significa que o caráter público da polícia não depende só de sua posição formal dentro do Estado, mas também de sua vinculação concreta à comunidade política e ao interesse coletivo.

O segundo atributo é a especialização, sendo considerado um termo relativo à exclusividade no desempenho de uma tarefa e que, no caso do policiamento, essa tarefa consiste na aplicação de força física no interior da comunidade (Bayley, 2002). Uma polícia especializada dedica sua atenção primária a essa função, ao contrário de arranjos institucionais em que autoridades administrativas, judiciais ou locais acumulam tarefas diversas, entre elas a manutenção da ordem. Essa observação é importante porque mostra que especialização não significa, necessariamente, monopólio absoluto da coerção, mas centralidade funcional da atividade policial.

Com isso, o autor quer demonstrar que a polícia moderna passa a existir como um órgão voltado principalmente para a preservação da ordem e para o uso legítimo da força em situações internas, em vez de exercer um conjunto amplo e misturado de atribuições. Diferentemente de contextos em que juízes, administradores locais ou outras autoridades também desempenham esse papel, aqui há uma concentração dessa missão em uma instituição própria. O ponto mais relevante é que essa característica indica um foco predominante de atuação, e não uma exclusividade total sobre toda forma de coerção existente na sociedade.

O terceiro atributo é a profissionalização, que Bayley (2002, p. 60-64) trata como uma característica distintivamente moderna, pois a profissionalização envolve preocupação explícita com a qualidade do desempenho policial, identificável por elementos como recrutamento com base em padrões específicos, remuneração apta a sustentar uma carreira, treinamento formal e supervisão sistemática. Com isso, a polícia deixa de ser apenas uma função exercida de modo episódico ou amador e se converte em uma carreira institucionalizada, com critérios internos de seleção, hierarquia e controle.

Em sentido mais amplo, trata-se da transformação dessa atividade em um ofício contínuo, exercido por pessoas admitidas segundo critérios definidos, preparadas de maneira sistemática e submetidas a acompanhamento institucional. A ideia central é que não se está mais diante de uma atuação improvisada ou ocasional,

mas de uma função estruturada como carreira, com regras de ingresso, formação específica, remuneração regular e controle interno do modo de atuação.

Esses três atributos ajudam a explicar por que o policiamento profissional se tornou tão influente. Ao reunir caráter público, especialização funcional e profissionalização organizacional, a polícia moderna passou a se apresentar como instituição capaz de exercer a coerção de maneira mais regular, estável e tecnicamente orientada. Em paralelo, a eficiência operacional ganhou centralidade crescente como critério de avaliação institucional, especialmente num cenário em que a polícia passou a ser cobrada por respostas mais rápidas, coordenação administrativa e capacidade de enfrentar a criminalidade urbana (Batitucci, 2019).

Ainda assim, o próprio argumento de Bayley (2002, p. 35-36, 50-51 e 64) impede que essa forma histórica seja tratada como natural ou como ponto final da evolução policial, posto que a combinação entre polícia pública, especializada e profissional não surgiu de maneira uniforme em todos os contextos, nem substituiu de forma definitiva outras modalidades de policiamento. Isso significa que o modelo profissional deve ser entendido como construção histórica contingente, e não como expressão inevitável de uma suposta racionalidade superior.

Essa historicidade é importante porque permite perceber que o policiamento profissional não equivale, automaticamente, ao bom policiamento. O fato de uma polícia ser pública, especializada e profissionalizada pode ampliar sua capacidade organizacional, mas não resolve, por si só, o problema da legitimidade do exercício de seu poder. Uma polícia pode ser tecnicamente bem estruturada e, ainda assim, operar de maneira opaca, pouco responsiva ou socialmente seletiva.

Foi em resposta a esse tipo de limite que ganharam espaço modelos que procuraram deslocar o eixo da avaliação policial. Um deles é o policiamento orientado para problemas. Nessa abordagem, a polícia deixa de ser pensada apenas como uma instituição que reage a ocorrências isoladas e passa a ser compreendida como organização que deve identificar problemas recorrentes, entender seus contextos e buscar respostas mais adequadas a eles (Batitucci, 2019).

Esse deslocamento é importante porque altera o próprio modo de compreender a função policial. Em vez de concentrar seus esforços apenas no atendimento imediato de episódios já consumados, essa perspectiva propõe uma atuação mais reflexiva, voltada à identificação de repetições, causas e circunstâncias que favorecem o surgimento de determinados conflitos. Com isso, a preocupação deixa

de recair apenas sobre o evento em si e passa a alcançar o ambiente em que ele se produz, permitindo intervenções menos improvisadas e potencialmente mais consistentes.

Além disso, essa forma de atuação sugere que a qualidade do trabalho policial não deve ser medida somente pelo volume de respostas oferecidas, mas também pela capacidade de compreender a natureza dos problemas enfrentados. Isso significa que agir bem não é apenas agir rápido, mas saber interpretar a situação, reconhecer seus fatores de permanência e escolher estratégias mais adequadas para enfrentá-la.

A relevância desse modelo está justamente em propor uma atuação menos mecânica e mais orientada pela análise concreta da realidade social sobre a qual a polícia intervém.

A interlocução de Brodeur com Herman Goldstein permite identificar com clareza esse aspecto. O policiamento orientado para a solução de problemas é apresentado como uma proposta de reconceituação mais abrangente da atividade policial, na medida em que desloca o foco para a variedade de problemas concretos enfrentados pelas corporações e exige um tratamento mais analítico dessas situações (Brodeur, 2002, p. 79). Não se trata, assim, de mera alteração de técnicas operacionais, mas de mudança mais profunda no modo de compreender a própria atuação policial.

Essa inflexão é decisiva porque rompe com a ideia de que a atividade policial possa ser avaliada apenas pela soma de suas rotinas ou pelo volume de suas intervenções. Aqui o policiamento não deve ser entendido como um fim em si mesmo, mas como um método para alcançar objetivos policiais mais amplos. A implicação disso é direta: não basta multiplicar ações, patrulhas, abordagens ou detenções; é preciso perguntar se tais meios de fato enfrentam o problema que justificou a intervenção.

Por isso, o policiamento orientado para problemas traz consigo uma crítica importante ao predomínio de avaliações centradas apenas em atividade institucional. Em vez de tomar a movimentação interna da organização como sinônimo de eficácia, esse modelo exige ligar os meios empregados aos fins perseguidos. Essa exigência torna mais difícil confundir desempenho operacional com qualidade institucional, como também. ajuda a mostrar o porquê do bom policiamento não se confundir com produtividade bruta (Brodeur, 2002, p. 57-59 e 68-69).

Outro modelo que ganhou relevo, sobretudo com o avanço das tecnologias de

informação, é o policiamento orientado por inteligência. Aqui, a ênfase recai sobre a coleta, o processamento, a análise e a disseminação de informações voltadas à definição de prioridades e à alocação de recursos. Em vez de reagir indistintamente a todos os eventos, a polícia passa a operar com seleção mais explícita de alvos, padrões e riscos (Silva *et al*., 2021).

Esse modelo de atuação parte do entendimento de que a atividade policial pode ser planejada de forma mais seletiva e estratégica, a partir do uso sistemático de informações consideradas relevantes para a definição de prioridades institucionais. Em vez de dispersar esforços em respostas homogêneas a toda e qualquer ocorrência, o policiamento orientado por inteligência busca identificar regularidades, conexões e fatores de risco que permitam direcionar a intervenção estatal para pontos considerados mais sensíveis (Silva *et al*., 2021). A informação, nesse contexto, deixa de ser mero elemento auxiliar e passa a desempenhar papel central na organização da atuação policial, influenciando tanto a leitura dos problemas quanto a distribuição de recursos e atenção.

Ao mesmo tempo, essa forma de policiamento também traz implicações importantes do ponto de vista normativo. Quanto maior a dependência de dados, sistemas de análise e critérios de seleção, maior a necessidade de examinar com cuidado como esses mecanismos são construídos e utilizados. Isso porque a definição de prioridades nunca é neutra, ela envolve escolhas sobre quais situações merecem maior vigilância, quais riscos são considerados mais relevantes e quais grupos ou territórios passam a ser mais intensamente observados (Oliveira, 2010). Por essa razão, o policiamento orientado por inteligência não pode ser avaliado apenas por sua capacidade de tornar a ação policial mais eficiente, mas também pela forma como lida com transparência, controle e justificativa institucional.

Esse modelo é importante porque desloca o centro da ação policial para a produção e o uso de conhecimento. No próprio Brodeur (2002, p. 79), aparece a observação de que o futuro do policiamento tende a depender crescentemente de informação, conhecimento e especialização, com a coleta, o processamento, a análise e a disseminação de informação ocupando lugar central.

Ao mesmo tempo, o policiamento orientado por inteligência não pode ser lido apenas como avanço técnico. Seu potencial de racionalização vem acompanhado de problemas específicos. A centralidade da informação torna mais sensível a discussão sobre transparência decisória, critérios de priorização, risco de seletividade e

capacidade de controle externo. O uso de estatísticas criminais e de dados para planejamento policial, como mostra a literatura brasileira, depende fortemente de cultura organizacional e de contexto institucional, não apenas da disponibilidade de informação (Azevedo; Riccio; Ruediger, 2011).

Sob outro ângulo, a incorporação de informação e análise ao trabalho policial não deve ser automaticamente tomada como sinal de aperfeiçoamento institucional. Ainda que esse modelo amplie a capacidade de planejamento e de definição de prioridades, ele também abre espaço para dúvidas quanto aos fundamentos das decisões, aos filtros utilizados para selecionar riscos e à possibilidade de supervisão externa.

Isso significa que a inteligência pode aumentar a capacidade analítica da polícia sem, por isso, resolver automaticamente os dilemas normativos do policiamento. Uma instituição pode se tornar mais sofisticada no uso de dados e, ao mesmo tempo, mais difícil de escrutinar publicamente. Pode também reforçar padrões anteriores de visibilidade seletiva, passando a tratar como prioridade aquilo que seus próprios sistemas capturam com maior facilidade. Por isso, a transição para modelos informacionais de policiamento exige atenção renovada aos mecanismos de *accountability* e aos critérios que orientam a seleção de riscos e alvos (Oliveira, 2010).

Essas transformações ajudam a explicar por que a ideia de policiamento democrático passou a ganhar importância como horizonte normativo mais abrangente. Diferentemente dos modelos anteriores, ele não se define apenas por uma técnica de atuação, mas por um conjunto de exigências quanto à relação entre polícia, lei, sociedade e poder público. A pergunta central deixa de ser apenas como a polícia opera e passa a incluir também sob quais controles, com quais justificações e em nome de que valores ela exerce sua autoridade.

O policiamento democrático pode ser entendido como uma forma de atuação policial submetida, de modo efetivo, aos princípios do Estado de Direito e à fiscalização pública. Mais do que designar um procedimento específico, essa noção expressa um padrão de relação entre polícia, sociedade e poder público em que a autoridade policial precisa estar vinculada à legalidade, à prestação de contas e à capacidade de responder às demandas da cidadania. Nessa perspectiva, a legitimidade da polícia não decorre apenas de sua aptidão para conter conflitos ou aplicar a lei, mas também da possibilidade de justificar suas decisões e de exercer seu poder sob controles institucionais e sociais reconhecíveis (Rocha, 2013).

A literatura brasileira tem insistido que o policiamento democrático depende de dimensões como *responsiveness* e *accountability.* Isto é, capacidade de responder ao público e capacidade de prestar contas de seus atos. Em texto especificamente voltado ao caso brasileiro, Rocha (2013) mostra que o debate sobre policiamento democrático está diretamente ligado a esses dois eixos, o que torna a legitimidade policial inseparável de mecanismos institucionais de controle e de resposta às expectativas sociais.

Em termos mais concretos, essa formulação indica que uma polícia democrática não pode se limitar a agir, ela precisa também manter relação de abertura e responsabilidade diante da sociedade. A ideia de *responsiveness* aponta para a necessidade de que a instituição seja sensível às demandas públicas, isto é, capaz de ouvir, compreender e responder de maneira adequada às necessidades e expectativas da população. Já a noção de *accountability* enfatiza que a atuação policial deve ser explicável, fiscalizável e passível de controle, o que significa que decisões, prioridades e usos da força não podem permanecer imunes ao escrutínio externo (Rocha, 2013). Em conjunto, essas duas dimensões mostram que o policiamento democrático depende não apenas da legalidade formal de sua atuação, mas também de sua capacidade de responder ao público e de justificar, perante ele, o modo como exerce sua autoridade.

O argumento é particularmente importante porque mostra que, em sociedades democráticas, a pluralização dos meios de controle e das estratégias policiais não pode ser acompanhada por opacidade institucional. Quanto mais variados e poderosos os instrumentos de policiamento, maior a necessidade de mecanismos que tornem suas ações inteligíveis e controláveis.

A discussão sobre legitimidade aprofunda esse ponto. Paula Poncioni (2022), ao tratar da legitimidade policial na democracia, reconstrói a importância da justiça procedimental e da confiança pública para a consolidação da autoridade policial. A relevância dessa abordagem está em mostrar que a obediência e a cooperação social não dependem apenas da capacidade de coerção, mas também da percepção de que a polícia age de forma justa, compreensível e respeitosa. Com isso, o bom policiamento deixa de ser pensado como mera soma de eficiência, profissionalização e capacidade técnica. Ele passa a ser compreendido como forma de exercício do poder policial que combina capacidade operacional com legalidade, controle, inteligibilidade e justificação pública. Essa mudança de eixo é decisiva porque impede

que o debate sobre modelos policiais seja capturado exclusivamente por métricas internas de desempenho.

5.1 POLICIAMENTO ENTRE CONTROLE POLÍTICO E VIGILÂNCIA AUTOMATIZADA

A polícia ocupa uma posição singular na vida política de uma nação porque é uma das instituições por meio das quais o poder público se torna concretamente perceptível na experiência cotidiana. Quando se fala em controle da polícia, não se está tratando apenas de administração interna, de comando hierárquico ou de disciplina corporativa. Trata-se, em sentido mais forte, de definir quem orienta o uso legítimo da força, em nome de quais finalidades e sob quais formas de responsabilização. Essa questão ganha densidade especial quando o policiamento passa a depender de sistemas de vigilância e tratamento massivo de dados, pois a expansão da capacidade técnica de observar e selecionar também amplia a necessidade de controle político e jurídico sobre a própria arquitetura da intervenção estatal.

Em “Padrões de Policiamento”, a polícia moderna aparece vinculada à combinação entre caráter público, especialização e profissionalização. Essa descrição, porém, não se reduz a um retrato organizacional. Ao afirmar que o policiamento é público quando é pago e dirigido pela comunidade que o autoriza, o livro introduz uma dimensão política decisiva, ou seja, a coerção só pode ser adequadamente compreendida quando permanece ligada a uma comunidade política e a formas reconhecíveis de direção coletiva. O ponto central não é apenas que a polícia integre o Estado, mas que sua atuação se mantenha vinculada ao interesse público e submetida a finalidades que possam ser justificadas politicamente (Bayley, 2002, p. 35-36 e 39).

Essa formulação permite perceber que o controle da polícia não se esgota na existência de um chefe de governo, de uma secretaria ou de uma cadeia de comando. Uma força policial pode estar formalmente subordinada ao Executivo e, ainda assim, operar com baixa transparência, forte opacidade decisória e fraca capacidade de controle externo. Por isso, a pergunta mais relevante não é apenas quem manda, mas como a autoridade policial é politicamente enquadrada, por quais normas ela se limita e de que modo suas escolhas podem ser publicamente examinadas. Quando o

controle é pensado apenas como comando vertical, perdem-se de vista os mecanismos democráticos de contenção do poder policial (Ribeiro, 2002).

A perspectiva histórica reforça esse argumento. O mesmo livro mostra que comunidades podem autorizar o uso da força e até desenvolver formas de governo sem, necessariamente, manter uma polícia pública moderna. Isso significa que a existência de ordem política e de autoridade jurídica não leva automaticamente ao surgimento de uma força estatal especializada (Bayley, 2002, p. 37-41 e 45). O policiamento, portanto, não é uma consequência natural da formação do Estado, mas uma escolha institucional sobre como organizar a coerção nos assuntos internos. E, sendo uma escolha, ele sempre envolve disputa sobre desenho institucional, repartição de poderes e formas de supervisão.

Essa historicidade ajuda a entender por que a polícia participa tão intensamente da vida política de uma nação. Ela não intervém apenas nos momentos extraordinários de crise, revolta ou comoção, mas também no cotidiano da circulação, da suspeição, da triagem de riscos e da definição prática de prioridades.

Em sociedades marcadas por desigualdade territorial e seletividade institucional, a polícia não apenas aplica uma ordem previamente dada, ela também ajuda a definir, na prática, quem será mais observado, quem será mais interpelado e quais espaços serão lidos como zonas de atenção reforçada. Por isso, sua atuação possui sempre uma dimensão distributiva e política, ainda quando se apresenta como simples cumprimento técnico da lei.

O tema se torna ainda mais sensível quando se observa a advertência formulada no debate sobre milícias, forças voluntárias e outras formas de coerção não plenamente públicas. A análise histórica mostra que, quando a aplicação da força reflete de maneira visível os interesses de grupos específicos, a ordem se torna abertamente política e perde legitimidade geral. Essa observação é valiosa porque revela que o problema do controle não se resume ao risco de abuso individual. O que está em jogo é impedir que a força organizada em nome da coletividade passe a traduzir preferências faccionais, econômicas ou territoriais de forma disfarçada. Em outros termos, controlar a polícia é também protegê-la contra sua transformação em instrumento particularizado de poder (Bayley, 2002; Oliveira, 2010).

É nesse ponto que a discussão sobre o futuro do policiamento adquire importância especial. A leitura de “Padrões de Policiamento” é particularmente instigante porque rejeita a ideia de que a trajetória de estatização e profissionalização

da polícia seja linear e irreversível. Ao contrário, o livro sustenta que a onda de profissionalização pode retroceder quando os recursos se tornam escassos ou quando mudam as circunstâncias nas quais a polícia tradicionalmente se apoia. Além disso, afirma que forças privadas de segurança tendem a ser, em geral, menos profissionalizadas que suas contrapartes públicas, e que formas de autodefesa mantidas por organizações voluntárias de cidadãos também reduzem o profissionalismo do policiamento (Bayley, 2002, p. 62).

Essa passagem é decisiva porque desfaz a imagem de um caminho inevitável rumo a uma polícia cada vez mais pública, especializada e profissional. O que se sugere, na verdade, é a possibilidade de um futuro marcado pela recomposição entre policiamento estatal, policiamento privado e iniciativas voluntárias de segurança. O policiamento público nessa chave, não elimina definitivamente seus concorrentes ou complementos, ele convive com eles, disputa espaço com eles e pode até perder centralidade em determinadas conjunturas. O futuro da polícia, portanto, não é apenas o futuro de uma organização, mas o futuro da própria distribuição social e institucional da segurança (Ribeiro, 2002).

Nessa perspectiva, o que se projeta não é o desaparecimento da polícia pública, mas sua convivência cada vez mais estreita com outros atores, outras infraestruturas e outras formas de vigilância. A análise de Bayley (2002), retomada por Ribeiro (2002), sugere que a estrutura dos sistemas nacionais de polícia tende a permanecer, mas, inserida em um ambiente mais complexo, marcado por maior especialização, mais tecnologia e maior presença de iniciativas privadas de segurança. Isso significa que o futuro do policiamento não será apenas mais estatal ou apenas mais técnico, ele será também mais híbrido. Em vez de monopolizar de modo absoluto a produção da ordem, a polícia pública tende a dividir espaço com empresas, sistemas automatizados, redes de informação e formas complementares de vigilância, o que desloca o debate para a forma como essas conexões serão governadas, supervisionadas e limitadas.

Esse ponto é especialmente relevante quando se observa a expansão de tecnologias como o *LPR*. Em contextos de leitura automática de placas, a pluralização do policiamento não aparece apenas na coexistência entre polícia pública e segurança privada em sentido clássico, mas também na dependência crescente de câmeras, *softwares*, bancos de dados, serviços de integração e dispositivos técnicos que frequentemente são produzidos, mantidos ou operados em arranjos institucionais

compartilhados.

Por isso, o futuro da polícia, nesse cenário, não diz respeito somente ao aumento de sua capacidade operacional, mas à transformação do próprio ambiente em que ela atua. Se a segurança passa a depender cada vez mais de informação circulando em redes técnicas e organizacionais amplas, o problema democrático deixa de ser apenas quem aborda, prende ou investiga, e passa a incluir quem coleta, quem processa, quem cruza e quem define o valor policial desses dados

A literatura recente sobre policiamento plural aprofunda esse diagnóstico ao mostrar que a segurança contemporânea já não é produzida exclusivamente pelo Estado. Empresas privadas, associações locais, centros de monitoramento, plataformas técnicas e redes de cooperação passam a participar da vigilância, da prevenção e da triagem de ameaças. Essa pluralização não representa apenas multiplicação de atores, ela altera a própria gramática do controle, porque decisões relevantes passam a surgir em zonas de contato entre esferas públicas e privadas. Com isso, o problema deixa de ser apenas quem exerce a coerção diretamente e passa a incluir quem fornece infraestrutura, quem seleciona critérios, quem define parâmetros de alerta e quem administra o fluxo de informação (Patriarca, 2023).

No caso do *LPR*, essa transformação aparece de maneira particularmente nítida. A leitura automática de placas não funciona apenas como instrumento de apoio visual ou como meio passivo de registro. Ela converte deslocamentos em informação consultável, circulação em sequência rastreável e a simples passagem por um ponto da cidade em ocorrência potencialmente relevante para a atuação policial. Na prática, isso significa que a vigilância deixa de depender apenas da presença física do agente na rua e passa a se organizar por meio de uma infraestrutura capaz de captar, processar, comparar e sinalizar dados em tempo real (IACP, [s.d.]). Por isso, o controle do policiamento, nesse cenário, não pode se limitar ao momento final da abordagem, devendo alcançar também listas de interesse, bases de dados conectadas, filtros de seleção e critérios que transformam uma placa em alerta.

A relevância política do LPR não decorre apenas de sua utilidade operacional, mas do tipo de poder que ele tende a expandir. Quando a circulação urbana se converte em trilha de dados, a polícia passa a dispor de meios mais sofisticados para seguir deslocamentos, reconstruir rotas e identificar regularidades. Isso produz ganhos evidentes de capacidade investigativa e de coordenação, mas também introduz um novo tipo de discricionariedade: a discricionariedade de vigilância, isto é,

a possibilidade de direcionar atenção policial não apenas com base em suspeitas individualizadas tradicionais, mas por meio de alertas, perfis e correlações produzidos a partir de grandes massas de informação. O resultado é uma ampliação qualitativa do poder policial, que passa a exigir mecanismos mais robustos de controle, fiscalização e prestação de contas.

Esse aspecto é especialmente importante porque o *LPR* opera em um ponto de convergência entre policiamento público e infraestrutura frequentemente privada. Câmeras, *softwares* de *OCR*, sistemas de armazenamento, bases integradas e interfaces de consulta podem ser fornecidos, operados ou calibrados por atores externos ao núcleo estatal tradicional. Isso não torna o policiamento automaticamente privado, mas o torna mais híbrido. E, quanto mais híbrida se torna a infraestrutura da segurança, mais difícil se torna identificar com precisão onde termina a decisão técnica e onde começa a decisão política. Em consequência, cresce a necessidade de regras claras sobre contratos, governança dos dados, tempos de retenção, auditoria de acessos e responsabilidade por erros ou abusos (Warren *et al*., 2013).

A literatura sobre vigilância viária e governança da privacidade ajuda a mostrar que tecnologias como *ANPR* não afetam apenas indivíduos pontualmente suspeitos, mas tendem a ampliar a capacidade de construção de perfis sobre populações inteiras em movimento. Quando o perfil se torna população, a triagem deixa de incidir apenas sobre casos singulares e passa a organizar o olhar institucional sobre fluxos amplos de circulação. Essa mudança é decisiva para uma dissertação que lida com videomonitoramento e *LPR*, porque o problema democrático deixa de ser apenas a legalidade do uso pontual da ferramenta e passa a envolver a forma como a infraestrutura de vigilância reordena a visibilidade da cidade e redistribui assimetricamente a atenção policial (DCAF, 2021).

Por isso, discutir o futuro do policiamento em chave democrática significa perguntar não apenas se a polícia do futuro será mais tecnológica, mas se continuará sendo adequadamente pública, controlável e justificável. A expansão do policiamento privado, a participação de organizações voluntárias e o uso intensivo de sistemas informacionais mostram que a estatização da polícia, além de não ser linear, pode se combinar com novas formas de dispersão do poder de vigiar. Nesse cenário, a legitimidade não depende apenas da finalidade declarada do sistema, mas da existência de mecanismos capazes de tornar o exercício da autoridade inteligível para o público, auditável por instâncias externas e limitado por normas que impeçam a

naturalização da suspeita automatizada.

Também por isso a discussão sobre controle político não pode ficar restrita ao momento visível da intervenção policial. Em ambientes atravessados por LPR, o controle democrático precisa alcançar etapas anteriores e menos perceptíveis, ou seja, a seleção do que será monitorado, os parâmetros de conexão entre bases, a definição das listas de observação, os protocolos de compartilhamento, os critérios de retenção e os procedimentos de revisão. O poder policial, nesse caso, já começa muito antes da abordagem, no desenho da própria infraestrutura que define o que será legível, prioritário e acionável. Falar em controle da polícia hoje, é também falar em controle de seus sistemas.

Em síntese, pensar o futuro do policiamento entre controle político e vigilância automatizada significa reconhecer que a transformação tecnológica da segurança pública não altera apenas os meios da ação policial, mas também reconfigura os problemas clássicos de legitimidade, direção institucional e limitação do poder. A expansão de infraestruturas como o LPR mostra que a polícia do futuro tende a ser mais informacional, mais conectada e mais dependente de redes técnicas e organizacionais complexas, nas quais se cruzam Estado, mercado e diferentes formas de produção da vigilância. Nesse cenário, o desafio central não está em saber apenas se a atuação policial será mais eficiente, mas em definir se ela continuará sendo adequadamente pública, politicamente controlável e juridicamente justificável. Por isso, o debate sobre o futuro do policiamento não pode ser dissociado da exigência de mecanismos robustos de supervisão, transparência, revisão e contenção democrática, capazes de impedir que a ampliação da capacidade de ver, rastrear e classificar, converta-se, silenciosamente, em ampliação ilegítima do poder de vigiar.

5.1.1 "Síndrome dos meios sobre os fins": LPR entre a métrica de atividade e o bom policiamento em Pernambuco

A incorporação de tecnologias de vigilância ao policiamento desloca o debate sobre legitimidade para um terreno particularmente sensível. Não se trata apenas de discutir se a polícia ganhou novas ferramentas, mas de examinar se a ampliação da capacidade de observar, rastrear e classificar continua submetida a fins públicos legítimos. Quando o videomonitoramento inteligente passa a integrar o núcleo da atuação policial, a avaliação do que seja bom policiamento já não pode repousar na

simples ideia de que mais tecnologia produz automaticamente melhor segurança.

Nesse contexto, a contribuição de Jean-Paul Brodeur é especialmente fecunda porque obriga a separar, com rigor, atividade institucional e produto final do policiamento. Ao discutir a avaliação de reformas policiais, ele mostra que organizações podem multiplicar programas, rotinas, dispositivos e indicadores sem que isso se converta necessariamente em melhora substantiva daquilo que importa ao público (Brodeur, 2002, p. 72 e 78). A advertência é decisiva para o seu objeto: sistemas de LPR e videomonitoramento tendem a gerar números em abundância, mas a existência desses números não resolve, por si, a pergunta sobre sua legitimidade democrática.

O ponto mais sensível dessa crítica está naquilo que o autor identifica como inversão entre meios e fins (Brodeur, 2002). Em vez de se perguntar se determinada estratégia realmente produz um resultado socialmente relevante, passa-se a valorizar a própria expansão da máquina institucional, ou seja, mais equipamentos, mais alertas, mais registros, mais painéis de controle, mais integração de dados. O problema, então, não é apenas metodológico, é político. Quando o aparato tecnológico se torna o centro da avaliação, o risco é que a tecnologia deixe de ser instrumento e passe a operar como justificativa de si mesma.

Essa inversão é particularmente provável em ambientes marcados por forte pressão governamental por resultados rápidos e visíveis. Tecnologias de vigilância oferecem precisamente esse tipo de visibilidade: instalações podem ser inauguradas, centrais de monitoramento podem ser exibidas, *dashboards* podem ser apresentados e números de atividade podem ser comunicados com grande facilidade. Tudo isso produz uma estética de modernização administrativa. Mas, boa parte dessa aparência de êxito diz respeito ao funcionamento interno do sistema e não necessariamente ao seu valor público. O fato de um sistema ser robusto, caro e tecnicamente sofisticado não demonstra, sozinho, que ele esteja produzindo bom policiamento.

É aqui que a noção de “síndrome dos meios sobre os fins” (Brodeur, 2002, p. 72) ganha força analítica. Em passagem particularmente esclarecedora, Brodeur (2002, p. 78) adverte para o risco de que certas reformas “[...] perpetue[m] a síndrome dos meios sobre os fins”. A formulação é curta, mas sua implicação é ampla. O sucesso institucional passa a ser medido pelo volume de atividade que a organização consegue produzir, e não pelo efeito final que sua atuação gera sobre os problemas que pretendia enfrentar.

Transposta para o videomonitoramento com *LPR*, essa crítica exige perguntar com muito cuidado o que, afinal, está sendo contado em Pernambuco. Se o êxito do sistema é apresentado sobretudo a partir da quantidade de câmeras contratadas ou instaladas, do número de placas lidas, dos incidentes captados, dos alertas emitidos e das ocorrências abertas, então a avaliação permanece fortemente ancorada em métricas de atividade[4]. Essas métricas podem ser úteis para demonstrar implantação e funcionamento, mas ainda não respondem à pergunta normativa sobre se a tecnologia está contribuindo para um policiamento melhor em sentido democrático (Pernambuco, 2025[5]).

Os materiais públicos localizados até aqui indicam precisamente essa predominância do plano operacional. A Secretaria de Estado de Defesa Social anunciou a assinatura do contrato para implantação de 2 mil câmeras com inteligência artificial e reconhecimento de placas, com investimento de R$ 122,9 milhões, apresentando a expansão da infraestrutura como avanço estratégico da capacidade de monitoramento e resposta (sds.pe.gov.br, 2024[6]) O Relatório Anual de Ações do Governo de Pernambuco de 2025, por sua vez, informa 916 pontos de captura de imagens e 393 câmeras ativas no ano, também com ênfase no dado de implantação e cobertura (Pernambuco, 2025). Esses registros mostram o crescimento do sistema, mas não constituem, por si, prova de impacto final sobre a segurança.

No mesmo sentido, a divulgação jornalística baseada em dados da própria Secretaria de Defesa Social informa que, em três meses, o novo sistema registrou 1.446 incidentes, média de 16 casos de interesse policial por dia, resultando em 185 ocorrências abertas e 11 prisões (Diário de Pernambuco, 2025[7]). Esses números revelam que o sistema produz acionamentos e apoia fluxos de trabalho. O que eles não demonstram, ao menos sem avaliação complementar, é se houve redução mensurável de crimes específicos diretamente relacionados ao uso do *LPR*, se os alertas gerados apresentaram boa qualidade analítica, ou se a tecnologia alterou

[4] Observe matéria veiculada pela Secretaria de Estado de Defesa Social de Pernambuco, que, no âmbito da política pública 'Juntos pela Segurança' instalou em 2025, cerca de 2 mil câmeras de videomonitoramento (Disponível em: https://www.sds.pe.gov.br/noticias/12076-juntos-pela-seguranca-governo-de-pernambuco-assina-contrato-para-instalacao-de-2-mil-cameras-de-videomonitoramento).
[5] No referido relatório consta a informação de instalação de 916 pontos de captura de imagens e 393 câmeras ativas em 2025.
[6] Reportagem disponível em: https://www.sds.pe.gov.br/noticias/12076-juntos-pela-seguranca-governo-de-pernambuco-assina-contrato-para-instalacao-de-2-mil-cameras-de-videomonitoramento.
[7]Reportagem disponível em: https://www.diariodepernambuco.com.br/vida-urbana/2025/12/11703745-novo-sistema-de-cameras-flagra-16-incidentes-por-dia-e-resulta-em-prisoes-em-pernambuco.html.

positivamente a experiência pública de segurança.

Essa diferença entre movimento interno e produto final é o centro do problema. Ler placas, gerar incidentes e abrir ocorrências são atividades. Reduzir roubos de veículos, localizar automóveis efetivamente vinculados a crimes com baixa taxa de erro, evitar revitimização, melhorar a capacidade de esclarecimento em situações delimitadas e aumentar a confiança pública já pertencem a outro plano. Brodeur (2002, p. 72 e 78) insiste que as dificuldades em aferir a eficácia de certos modelos "[...] no que se refere ao seu produto final, são bem reais". A observação vale integralmente para a vigilância automatizada, pois quanto mais o sistema produz atividade facilmente quantificável, mais necessário se torna distinguir o que é mera produtividade do que é resultado socialmente relevante.

A questão, portanto, não é negar utilidade ao videomonitoramento. Em situações concretas, sistemas de câmeras e leitura automática de placas podem apoiar investigações, acelerar a localização de veículos e ampliar a capacidade de reconstrução de trajetórias. O ponto crítico é outro, haja vista que um instrumento eventualmente útil não se torna, por isso, autojustificável. O bom policiamento exige que a tecnologia permaneça subordinada a finalidades delimitadas e avaliáveis, e não que essas finalidades sejam presumidas apenas porque a ferramenta existe, funciona e produz números expressivos (Brodeur, 2002, p. 72 e 78).

Essa exigência é especialmente importante porque o videomonitoramento com *LPR* altera a própria temporalidade do policiamento. Em vez de atuar apenas após um fato consumado, a infraestrutura passa a acompanhar fluxos, reter rastros e sinalizar relevâncias operacionais em tempo quase contínuo. Isso amplia a capacidade estatal de reação e de coordenação, mas também reorganiza as bases sobre as quais a atenção policial é distribuída. A questão democrática deixa de ser apenas se a polícia pode usar a força numa abordagem e passa a incluir quem entra em listas, quais trajetos se tornam mais legíveis, quais cruzamentos geram alertas e quais eventos são convertidos em prioridade institucional (Joh, 2016).

Em termos mais simples, isso significa que o *LPR* muda não apenas a intensidade da vigilância, mas também o momento em que o poder policial começa a agir. A polícia deixa de depender apenas de uma ocorrência já consumada ou de uma abordagem presencial e passa a operar com informações geradas continuamente sobre deslocamentos e passagens pela cidade. Com isso, a discussão democrática não se limita mais ao uso da força no instante final da intervenção, mas precisa

alcançar também as etapas anteriores, isto é, os critérios que definem quem será monitorado, quais trajetos chamarão atenção e quais dados serão transformados em alerta e prioridade policial.

Nesse cenário, a “síndrome dos meios” pode se aprofundar justamente porque a própria arquitetura tecnológica estimula a contagem de tudo o que circula por ela. Placas lidas, consultas realizadas, alertas disparados, imagens recuperadas, tempo de resposta, áreas cobertas, integrações realizadas, todos esses elementos podem ser mensurados com relativa facilidade. A consequência é a tentação de tratar a expansão da capacidade de medir e de vigiar como prova bastante do sucesso do sistema. Mas, uma polícia mais capaz de contar não é, por isso, uma polícia melhor. Sem critérios externos ao próprio funcionamento da ferramenta, a avaliação corre o risco de permanecer prisioneira da lógica interna do dispositivo.

A dificuldade é ainda maior porque o videomonitoramento não produz apenas informação, ele também produz seleção. Quando um sistema automatizado define ocorrências de interesse, transforma passagens em eventos, converte circulação em trilha consultável e aciona respostas policiais, ele participa ativamente da distribuição da visibilidade estatal. Não está apenas registrando o real, está também classificando o que será tratado como relevante. Por isso, a avaliação democrática do *LPR* não pode se limitar a perguntar quantos alertas surgiram, mas deve indagar quais critérios os estruturam, quem os revisa e quais grupos ou territórios podem ser mais intensamente atingidos por esse desenho (Warren *et al*., 2013).

O ponto aqui é que o *LPR* não age só como uma câmera que registra o que passa. Quando ele lê placas, cruza informações e gera alertas, ele também ajuda a decidir o que vai chamar a atenção da polícia. Então, além de captar a circulação, o sistema passa a destacar certos veículos, certos trajetos e certos movimentos como mais importantes do que outros. É por isso que a discussão não deve ficar restrita ao número de alertas emitidos, mas precisa alcançar os critérios que fazem alguns deslocamentos se tornarem mais visíveis para o Estado do que outros.

Isso ajuda a perceber que o resultado relevante de um sistema como o *LPR* não pode ser medido apenas pelo número de prisões, apreensões ou ocorrências abertas. Há um plano mais amplo, que envolve a confiança que a população deposita na polícia, a percepção de que as decisões são justas, a possibilidade de compreender como o sistema funciona e, sobretudo, a existência de meios para contestar erros, excessos ou tratamentos desiguais. Uma tecnologia pode, ao mesmo

tempo, ampliar a capacidade de intervenção estatal e enfraquecer a legitimidade da instituição, caso opere com baixa transparência, critérios pouco inteligíveis ou efeitos seletivos desproporcionais (Poncioni, 2022).

É justamente por isso que a literatura sobre legitimidade policial chama atenção para algo que nem sempre aparece nos discursos sobre inovação, isto é, a qualidade da atuação policial não depende apenas de sua eficiência instrumental. Ela também depende da forma como essa atuação se apresenta ao público, dos critérios que a sustentam e da possibilidade de prestar contas sobre suas escolhas e seus procedimentos (Poncioni, 2022). Em outras palavras, uma polícia pode até agir mais rapidamente e com mais informação, mas isso não basta para que sua atuação seja percebida como justa, aceitável e democraticamente legítima.

A pergunta que se impõe então é bastante direta: no caso pernambucano, há demonstração pública de que o *LPR* tenha reduzido, de forma verificável, crimes específicos para os quais foi apresentado como ferramenta útil? Há evidências acessíveis de que o sistema tenha aumentado a confiança da população na polícia, reduzido arbitrariedades ou melhorado a percepção de justiça no uso da vigilância? Com base nos materiais públicos localizados até aqui, essa demonstração ainda não aparece de forma clara (sds.pe.gov.br, 2024; Pernambuco, 2025; Diário de Pernambuco, 2025). O que se encontra com mais nitidez são indicadores de implantação, expansão da infraestrutura e volume de acionamentos produzidos pelo sistema.

Essa insuficiência não deve ser confundida automaticamente com prova de fracasso. O ponto é outro. A publicidade institucional do sistema parece estar muito mais assentada no terreno dos meios do que no terreno dos fins. É exatamente nesse tipo de situação que a crítica de Brodeur (2002) se torna mais exigente. Não basta exibir câmeras instaladas, incidentes captados ou prisões apoiadas pela tecnologia, é preciso demonstrar em que medida o sistema enfrenta problemas públicos claramente definidos, com quais custos, sob quais salvaguardas e com quais resultados verificáveis para além da intensificação da atividade policial (Brodeur, 2002, p. 72 e 78). Por isso que a ideia do bom policiamento exige uma mudança de foco, em vez de celebrar automaticamente o aumento da capacidade de leitura, cruzamento e sinalização, a avaliação deve perguntar se a tecnologia é realmente necessária para o problema que pretende enfrentar, se seu uso é proporcional ao grau de intrusão que produz e, se haveria alternativas menos gravosas para alcançar fins semelhantes. A

discussão, então, deixa de ser apenas quantitativa e passa a ser propriamente normativa. O que importa não é apenas o quanto o sistema faz, mas se ele faz o que deve fazer dentro dos limites do que pode legitimamente fazer.

Essa inflexão é importante porque impede que a técnica passe a ocupar o lugar da justificação. Em políticas orientadas pela linguagem da inovação existe sempre o risco de que a simples presença de uma ferramenta sofisticada funcione como prova implícita de validade, em outros termos, se o sistema é moderno, integrado e inteligente, presume-se que também seja legítimo. Mas a legitimidade não nasce da sofisticação da ferramenta, ela depende da finalidade a que o sistema serve, dos limites que condicionam seu uso, dos mecanismos de controle que o cercam e da publicidade dos critérios que organizam seu funcionamento. Uma tecnologia pode ser altamente precisa no plano operacional e, ainda assim, ser mal-governada do ponto de vista democrático (Poncioni, 2022).

É por isso que a exigência de evidência precisa ser levada a sério. Não basta reunir dados sobre o que o sistema faz internamente, é necessário saber o que ele produz externamente, para quem, com quais efeitos e com quais assimetrias. Uma avaliação democrática do videomonitoramento com *LPR* deveria, por exemplo, distinguir ocorrências meramente registradas de resultados substantivos, aferir o peso de falsos positivos, examinar a distribuição territorial dos acionamentos e verificar se houve impacto real sobre problemas criminais previamente delimitados. Sem esse tipo de demonstração, permanece-se no terreno da promessa e não da comprovação.

Nesse ponto, a advertência de Brodeur é especialmente precisa. Segundo Brodeur (2002, p. 78), há “um risco genuíno” de se perpetuar a “síndrome dos meios sobre os fins”. A formulação é importante porque desloca o foco da simples produtividade para a relação entre resposta institucional e problema público efetivamente enfrentado. O que está em questão não é apenas o quanto o sistema opera, mas se aquilo que ele produz se traduz de fato em resultado socialmente relevante.

No caso pernambucano, essa crítica ajuda a recolocar a questão em seus termos mais rigorosos. O ponto decisivo não é saber se o sistema lê muito, alerta muito ou cobre muito. O que realmente importa é saber se essa ampliação de capacidade permanece subordinada a fins públicos demonstráveis, a controles robustos e a padrões de legitimidade compatíveis com a democracia. Quando à avaliação permanece concentrada em infraestrutura, registros e acionamentos, corre-

se o risco de legitimar a expansão da vigilância apenas porque ela gera números, sem demonstrar com a mesma clareza seus efeitos sobre os problemas que justificaram sua adoção. Por essa razão, o bom policiamento exige uma pergunta mais exigente do que aquela sugerida pela retórica da inovação. O problema não é simplesmente saber se o LPR funciona, mas se ele funciona para fins legítimos, com resultados socialmente relevantes e sob condições institucionais que permitam controle, crítica e revisão. A principal contribuição de Brodeur (2002), aqui, está em lembrar que a tecnologia não pode se converter em fim em si mesma. Em ambientes de vigilância automatizada, resistir à “síndrome dos meios sobre os fins” é condição para que a segurança pública não se afaste de seus compromissos democráticos.

5.2 RASTREABILIDADE E CONTROLE EXTERNO DO LPR.

A incorporação de IA ao videomonitoramento só pode ser compreendida do ponto de vista democrático, se o debate deslocar o foco do “que a tecnologia faz” para “como o poder se organiza quando a tecnologia passa a orientar decisões”. Em sistemas como o *LPR*, a decisão relevante não é apenas a leitura automática da placa, mas a cadeia institucional que transforma um registro em alerta, o alerta em prioridade operacional e a prioridade em abordagem, diligência, investigação ou prova. Por isso, falar de responsabilização é falar de imputação: em que ponto o Estado assume, de modo verificável, quem autorizou, quem consultou, quem decidiu e quem responde quando o uso do sistema produz erro, abuso, seletividade territorial ou desvio de finalidade (Bioni; Garrote; Guedes, 2023).

A pergunta “quem responde?” costuma ficar nebulosa quando decisões são “apoiadas” por IA, porque os atores se multiplicam, pois quem contrata e define requisitos, quem configura parâmetros, quem administra acessos, quem opera a central, quem aciona a equipe em campo, e quem valida o resultado? No caso pernambucano, o próprio Termo de Referência já reconhece que não se trata apenas de equipamentos, mas de uma plataforma com regras de acesso, operação e conformidade, mencionando controles lógicos e físicos, classificação de informação e requisitos de segurança e transparência vinculados à LGPD (Pernambuco, 2024). Isso é um ponto importante metodologicamente, uma vez que o Estado não está apenas “instalando câmeras”, mas criando uma infraestrutura informacional que exige

desenho de governança, porque a forma de operar essa infraestrutura define o grau de discricionariedade real no uso dos dados.

Esse ponto se torna ainda mais delicado quando se leva a sério a advertência de Bayley (2002, p.46): “[...] as formas de policiamento público não suplantam permanentemente as privadas; este processo é reversível”. A observação é particularmente útil para o *LPR* porque mostra que a segurança contemporânea não se organiza apenas dentro dos limites clássicos da polícia estatal. Quando a captura, o processamento e a classificação dos dados dependem de *softwares*, plataformas, rotinas de integração e parâmetros definidos em ambientes técnico-privados, a atuação policial passa a operar em um terreno híbrido. O problema não é apenas que existam prestadores privados participando da infraestrutura, mas que essa participação possa deslocar de forma pouco visível, o centro de decisões relevantes sobre o que será visto, sinalizado e tratado como prioridade. Assim, embora a decisão final continue formalmente atribuída ao Estado, parte importante do enquadramento do real já pode ter sido moldada por escolhas técnicas que não passaram pelo mesmo grau de escrutínio público exigido das decisões propriamente políticas.

É justamente aí que a pergunta “quem responde?” ganha densidade democrática. Se, como o próprio Bayley (2002, p. 35-36) sustenta: o policiamento público é aquele que é “[...] pago por e controlado pelas comunidades, agindo coletivamente”, então a expansão de infraestruturas privadas no núcleo da vigilância não pode ser tratada como detalhe meramente operacional. Quando a empresa define parâmetros, ajusta filtros, desenha regras de acesso, estrutura categorias de alerta ou condiciona o modo como os dados circulam, há o risco de que a decisão técnica passe a substituir, na prática, a decisão política do Estado, sem que isso apareça claramente como escolha sujeita a controle público.

Nesse tipo de arranjo, a responsabilidade tende a se fragmentar: o Estado pode alegar que apenas utiliza a ferramenta; a empresa pode dizer que apenas executa especificações; e, no meio desse circuito, torna-se mais difícil localizar quem efetivamente definiu os critérios que produziram determinada visibilidade, determinado alerta ou determinada intervenção. A hibridização do policiamento aludida no livro, assim, não elimina a responsabilidade estatal, mas pode obscurecê-la, criando um espaço cinzento em que o poder de selecionar e classificar circula com intensidade crescente e com transparência decrescente (Bayley, 2002, p. 50).

Nesse desenho, a auditabilidade aparece como condição de possibilidade do controle democrático. O documento licitatório de Pernambuco exige que o sistema permita "*logs* de acesso e auditoria de todas as ações do usuário" e, em outra seção, afirma expressamente que "toda a plataforma deve ser auditável", destacando que um dos principais itens da auditoria serão os "*logs* de acesso ao sistema e atividade na plataforma", para identificar "quem acessou o sistema" e "realizou determinada ação", visando garantir autenticidade e confidencialidade dos dados (Pernambuco, 2024). Essa exigência não é detalhe técnico: ela define se o poder de consulta e acionamento será rastreável. Sem logs confiáveis, não há como reconstruir a trajetória decisória de um alerta ou de uma busca, o que inviabiliza responsabilização administrativa, civil, disciplinar e, também, o controle externo.

Esse ponto pode ser aprofundado a partir da crítica, já citada, de Brodeur (2002, p. 72 e 78) à "síndrome dos meios sobre os fins". Se o *log* se limita a registrar que houve uma consulta, quem acessou o sistema e em que horário, ele continua operando sobretudo no plano da atividade institucional. Isso é importante, mas ainda insuficiente. Para que a auditabilidade tenha valor democrático real, os registros precisam permitir reconstruir não apenas o acesso, mas a justificativa substantiva da intervenção: porque aquele dado foi consultado, em conexão com qual situação concreta, com qual finalidade pública e com qual efeito posterior. Do contrário, a rastreabilidade corre o risco de reproduzir exatamente o problema apontado em "Como reconhecer um bom policiamento*"*: muita visibilidade sobre os meios e pouca inteligibilidade sobre os fins. Em vez de servir à avaliação do "produto externo do policiamento", o *log* passa a funcionar apenas como contador de uso da máquina, perpetuando a lógica pela qual o aparato comprova sua própria atividade sem demonstrar, com a mesma clareza, a relevância pública de suas decisões (Brodeur, 2002, p. 72 e 78).

Além disso, a governança de acesso é parte do próprio problema jurídico. O Termo de Referência prevê gestão de perfis de acesso e descreve o controle de acesso como mecanismo para assegurar que apenas usuários autorizados acessem recursos, estabelecendo identificação única e regras para que cada pessoa acesse "somente ao que é necessário" para realizar o trabalho. Em plataformas que integram *LPR* e análise de vídeo, isso é crucial porque o dano potencial não está apenas na captura, mas na consulta e no cruzamento. A possibilidade de buscar placas, aplicar filtros, recuperar trajetos e correlacionar ocorrências transforma o acervo em

ferramenta de investigação e inteligência; por isso, a gestão de perfis e privilégios precisa ser tratada como salvaguarda democrática, não como mera conveniência operacional (Pernambuco, 2024).

A responsabilização também depende de como se definem e se governam os "seletores" internos do sistema, isto é, listas, parâmetros de correspondência, limiares de alerta, regras de retenção e critérios de consulta. O Termo de Referência pernambucano aponta tarefas como "analisar *logs*" e administrar controle de acesso no escopo de operação/gestão do sistema, o que evidencia que o sistema cria funções permanentes de administração e supervisão (Pernambuco, 2024). Em termos práticos, isso significa que o "centro" da decisão pode migrar do agente que aborda para quem configura e administra o que será visto como evento relevante. O problema jurídico, então, não é apenas punir o abuso após o fato, mas desenhar procedimentos para que a configuração do sistema seja rastreável, revisável e submetida a justificativas públicas quando produzir efeitos sobre abordagens e investigações.

O vínculo com as "zonas de exceção", do art. 4º da Lei Geral de Proteção de Dados (LGPD), torna esse ponto ainda mais sensível. A LGPD exclui de seu escopo, em regra, tratamentos para fins de segurança pública e investigação penal, o que cria um espaço normativo em que a disciplina geral de direitos e deveres não se aplica automaticamente (Brasil, 2018). Ao mesmo tempo, a própria Autoridade Nacional de Proteção de Dados (ANPD) tem reconhecido, em documentos técnicos (Nota Técnica nº 29/2024), que há competências e possibilidades de orientação técnica relacionadas ao art. 4º, ainda que a arquitetura jurídica seja incompleta e dependa de marco específico (Brasil, 2024). Essa combinação produz um cenário típico de risco institucional: a tecnologia avança e se consolida como infraestrutura, enquanto as garantias ficam dispersas, fragmentadas ou dependentes de escolhas internas da administração.

É exatamente por isso que "auditabilidade" precisa ser mais do que "ter *logs*": ela precisa ser desenhada para permitir controle externo real. Um *log* útil para a democracia não é apenas um registro interno*,* ele precisa ser íntegro, preservado, correlacionável com eventos e capaz de sustentar reconstituição independente do que ocorreu. A literatura brasileira recente sobre vigilância e justiça criminal tem chamado atenção para o fato de que, sem governança robusta, tecnologias podem concentrar poder informacional na própria instituição que as utiliza, dificultando escrutínio por órgãos externos e pela sociedade (Ramos, [s.d]). Nessa chave, a exigência do Termo

de Referência (Pernambuco, 2024) de que a plataforma seja auditável é um ponto de partida, mas não encerra a discussão: o que importa é quem audita, com que periodicidade, com quais critérios, e o que acontece quando a auditoria encontra uso indevido.

A necessidade de controle externo tem base constitucional e institucional no Brasil, especialmente pela atribuição do Ministério Público de exercer controle externo da atividade policial. Normas recentes do Conselho Nacional do Ministério Público (CNMP) reforçam atribuições e diretrizes desse controle, o que abre uma via concreta para pensar tecnologias, porque se a atividade policial passa a ser orientada por alertas e buscas em sistemas, o controle externo precisa ter condições de fiscalizar o uso desses sistemas, inclusive a partir de registros, trilhas de auditoria e protocolos de acionamento (CNMP, 2023).

Desta forma, a participação do Ministério Público no controle externo da atividade policial não pode ser pensada apenas em termos formais, como se bastasse a previsão constitucional ou a existência de uma resolução do CNMP para que a fiscalização se torne efetiva. Em sistemas como o *LPR*, o controle depende de condições materiais e técnicas para examinar trilhas de auditoria, compreender metadados, verificar regras de acesso, reconstruir fluxos de consulta e identificar se determinada busca ou alerta foi compatível com a finalidade pública declarada. Se o órgão de controle não dispõe de acesso tempestivo aos registros relevantes, nem de capacidade técnica para interpretar o funcionamento da plataforma, a auditabilidade corre o risco de permanecer apenas potencial. A própria Resolução CNMP n. 279/2023 reforça que o controle externo alcança a regularidade, a adequação e a eficiência da atividade policial, o que, em contextos de vigilância algorítmica, exige mais do que controle documental retrospectivo: exige capacidade de fiscalização informada sobre a infraestrutura que organiza a decisão (CNMP, 2023). Esse ponto pode ser iluminado pela experiência portuguesa, em que a videovigilância em espaço público foi sendo estruturada não como simples opção gerencial das forças de segurança, mas como resultado de um arranjo prático entre autorizações, pareceres, proteção de dados e competências institucionais (CNMP, 2023). Estudos sobre os 20 anos de videovigilância em Portugal mostram justamente que o controle não se resolve por uma autorização abstrata, mas por uma rede de procedimentos, órgãos e disputas concretas em torno de critérios, prazos e competências, o que ajuda a perceber que,

no caso brasileiro, logs e rastreabilidade só ganham efetividade democrática quando inseridos em um circuito real de fiscalização externa (Melo; Viseu, 2024).

A utilidade da comparação com Portugal está em mostrar, de modo bem “concreto”, como a governança da videovigilância em espaço público tende a ser construída como um encadeamento jurídico-institucional e não apenas como escolha interna da administração. No regime português, a própria lógica de instalação e funcionamento de sistemas de videovigilância, especialmente com câmaras fixas, é estruturada por atos de autorização e por parecer prévio da autoridade de proteção de dados, de forma que limites de finalidade, requisitos de segurança do tratamento e previsibilidade legal aparecem como condições do regime e não como boas práticas voluntárias (Portugal, 2021). Esse desenho é reforçado pelas orientações públicas da Comissão Nacional de Proteção de Dados (CNPD), que tratam a videovigilância como matéria sujeita a requisitos legais e a um conjunto de cuidados de conformidade, e, portanto, inserem a discussão no plano da legalidade e da fiscalização, e não apenas da eficiência técnica (CNPD, [s.d.]). Ao mesmo tempo, estudos recentes sobre a trajetória da videovigilância em Portugal indicam que esse arranjo não elimina conflitos; ao contrário, descrevem a expansão progressiva do dispositivo e registram tensões e disputas institucionais em torno de autorizações, critérios e competências, o que é particularmente útil para o caso brasileiro porque evidencia que “controle” não é apenas ter uma norma em abstrato, mas sustentar, na prática, um arranjo entre órgãos, procedimentos, competências e rotinas de supervisão capaz de acompanhar a expansão tecnológica (Melo; Viseu, 2024).

O ponto não é deslocar a gestão técnica para fora da polícia, mas garantir que existam condições materiais e normativas para fiscalização independente, sobretudo quando a tecnologia aumenta a capacidade de rastrear a vida cotidiana.

Um risco recorrente, reconhecido na literatura sobre governança de tecnologia no setor público, é o desvio de finalidade e a expansão progressiva do sistema. Em plataformas integradas, usos inicialmente vinculados a roubo de veículos e investigação podem migrar para finalidades laterais, com novos órgãos acessando dados, novos cruzamentos sendo habilitados e prazos de retenção sendo ampliados “por precaução”. Esse tipo de expansão é mais fácil quando a infraestrutura já está instalada e quando o sistema opera como serviço contínuo. O Termo de Referência pernambucano chega a mencionar a importância de transparência e regras claras, inclusive em hipóteses de compartilhamento de dados com entidades privadas,

fazendo remissões a dispositivos da LGPD sobre transparência e tratamento pelo poder público. Essa passagem é relevante porque mostra que a própria contratação reconhece o problema do fluxo de dados, e, portanto, reforça a necessidade de salvaguardas formais sobre compartilhamento, finalidades e responsabilização (Pernambuco, 2024).

Na perspectiva de políticas públicas, isso se conecta diretamente ao seu objeto empírico. Em Pernambuco, a implantação descrita no processo licitatório estrutura centros, integrações e funcionalidades analíticas, incluindo *LPR* e exigências de *logs* e auditoria (Pernambuco, 2024). A pergunta que o capítulo precisa sustentar, sem recorrer a conjecturas, é: quais dispositivos de controle acompanham essa expansão para que o ganho investigativo não gere um déficit democrático. Isso envolve, minimamente, quatro camadas: rastreabilidade técnica (*logs* íntegros e completos), justificabilidade procedimental (registro de motivo e finalidade em consultas e acionamentos), auditoria independente (interna e externa, com capacidade real de examinar trilhas e protocolos) e transparência mínima (informação pública sobre finalidade, regras de uso, retenção, compartilhamento e mecanismos de fiscalização) (CNMP, 2023).

No Brasil, a lacuna de um marco específico para dados em segurança pública foi justamente o que motivou discussões e anteprojetos voltados a criar uma “LGPD penal” ou regime próprio para tratamento de dados em investigação e segurança, reconhecendo que a exclusão do art. 4º não resolve o problema, apenas o desloca (Congresso Nacional, 2020). Para esta dissertação, esse pano de fundo tem uma função metodológica: ajudar a justificar por que “zonas de exceção” não podem significar “zonas sem governança”. A ausência de um regime específico robusto aumenta o peso das salvaguardas contratuais, procedimentais e institucionais no plano local, inclusive em contratações públicas que já preveem auditabilidade e controle de acesso como requisitos.

Por fim, responsabilização não é apenas atribuir culpa após um dano, mas criar condições para que danos sejam prevenidos e para que o exercício do poder seja verificável. Em sistemas de IA no policiamento com utilização do *LPR*, o ponto mais sensível é evitar que a decisão se “dissolva” entre máquina, operador e instituição, tornando impossível identificar o fundamento do ato. O Termo de Referência pernambucano oferece elementos concretos para sustentar que a governança já foi reconhecida como requisito do sistema, ao exigir *logs*, auditoria e controle de acesso

(Pernambuco, 2024). O passo seguinte, em termos de compatibilidade democrática, é amarrar esses requisitos a controles externos e mecanismos de contestação, para que a tecnologia não opere dentro de uma exceção permanente e opaca, mas sob regras públicas, verificáveis e responsabilizáveis.

5.3 PARÂMETROS PARA UM MODELO DE LEGITIMIDADE DEMOCRÁTICA NA VIGILÂNCIA

A etapa final desta dissertação exige um deslocamento do plano descritivo para o plano normativo. Depois de reconstruir a arquitetura técnico-institucional do videomonitoramento com leitura automática de placas em Pernambuco e de examinar seus problemas de proporcionalidade, responsabilização e controle, a questão que permanece é outra: em que condições esse uso pode ser considerado democraticamente legítimo? Não se trata de perguntar apenas se a tecnologia funciona, mas se seu funcionamento está submetido a critérios públicos que a tornem justificável perante a coletividade.

A legitimidade democrática, nesse contexto, não nasce da sofisticação técnica da IA, nem da simples ampliação da capacidade estatal de observar e agir. Ela depende de uma combinação mais exigente entre capacidade operacional, legalidade, limitação do poder, controle externo e inteligibilidade pública dos critérios de uso. Em matéria de policiamento, isso significa reconhecer que eficiência e legitimidade não são sinônimas. Um sistema pode ser rápido, preciso e amplamente integrado e, ainda assim, operar de forma opaca, seletiva ou insuficientemente controlável (Brodeur, 2002, p. 72 e 78).

Se o “bom policiamento”, como se viu, exige que os meios permaneçam subordinados aos fins públicos e ao escrutínio democrático, o uso do *LPR* em Pernambuco só pode ser defendido como compatível com esse ideal se estiver inserido em uma estrutura de governança capaz de responder a três perguntas fundamentais. A primeira diz respeito ao território, tendo em vista como a tecnologia redistribui a visibilidade da cidade e com que efeitos sobre a produção da suspeição. A segunda diz respeito à responsabilidade de quem controla a arquitetura técnica e como o Direito enquadra decisões apoiadas por IA. A terceira diz respeito ao resultado social, apurando se o sistema efetivamente melhora a segurança e a confiança

pública, ou se apenas multiplica métricas de atividade. A proposta desta seção é, justamente, organizar esses parâmetros em três eixos complementares.

As três dimensões desenvolvidas a seguir não são apresentadas aqui como um modelo fechado extraído de uma única obra, mas como uma sistematização analítica proposta nesta dissertação, construída a partir do diálogo entre o referencial de "bom policiamento", a literatura sobre vigilância contemporânea, os debates sobre policiamento democrático e a reconstrução documental do caso pernambucano. A dimensão territorial decorre da constatação de que o *LPR* reorganiza desigualmente a visibilidade da cidade e produz efeitos sobre fluxos, espaços e suspeições; a dimensão da responsabilização resulta da necessidade de submeter a infraestrutura técnica a regras públicas de auditabilidade, controle e imputação de responsabilidade; e a dimensão da eficácia social nasce da exigência de que o sistema seja avaliado não apenas por sua atividade interna, mas por seus efeitos públicos verificáveis sobre segurança, confiança e justiça. O que se propõe, portanto, não é uma tipologia abstrata, mas uma forma de organizar, em chave normativa, os principais problemas revelados pela implantação do *LPR* em Pernambuco, transformando os achados da pesquisa em critérios para avaliar sua justificação democrática.

5.3.1 Legitimidade territorial: da "fobópole" à geografia da suspeição

A primeira possível dimensão da legitimidade democrática do *LPR* é o critério territorial. A vigilância não se distribui de modo neutro pela cidade. Ela é instalada, concentrada e operada segundo prioridades que transformam alguns espaços em áreas de observação reforçada e deixam outros sob menor densidade de atenção. No caso pernambucano, o desenho projetado no Termo de Referência prevê 1.347 Pontos de Captura de Imagem, com 378 câmeras dotadas de leitura automática de placas, distribuídos entre centros de gerenciamento no Recife, em Caruaru e em Petrolina (Pernambuco, 2024). Essa distribuição já revela, por si, que a vigilância não se limita a "cobrir" o território, ela o hierarquiza.

Isso significa que o sistema não apenas acompanha o espaço urbano, ele o reorganiza como superfície de legibilidade desigual. Corredores de fluxo, entradas e saídas metropolitanas, vias estratégicas e áreas mais fortemente conectadas à malha de monitoramento tornam-se mais captáveis, mais pesquisáveis e mais suscetíveis de acionamento. A questão democrática começa antes da abordagem individual,

porque ela já está presente na própria decisão sobre onde a infraestrutura vai “ver” mais e onde ela verá menos. Quando o Estado define quais circuitos serão transformados em zonas de vigilância intensiva, ele define também onde a circulação será mais facilmente convertida em dado policial.

É justamente nesse sentido que a implantação do *LPR* em Pernambuco pode ser lida como questão de territorialidade política. Ainda que não tenha sido realizado, nesta pesquisa, um mapeamento geográfico exaustivo da posição de cada câmera, os elementos levantados por fontes públicas já permitem afirmar que a distribuição dessa tecnologia não constitui ato puramente técnico ou neutro. Ao definir pontos de captura, eixos de circulação prioritários e áreas de maior densidade de monitoramento, o Estado também define como pretende governar o espaço urbano e administrar seus fluxos.

A contribuição de Rogério Haesbaert aprofunda esse diagnóstico porque ajuda a romper com uma visão mais estática do território, entendido apenas como superfície contínua, fechada e claramente delimitada. Em “Territórios alternativos”, o autor mostra que território e rede não devem ser tratados como realidades opostas, mas como dimensões que se articulam. Em passagem particularmente útil para esta dissertação, ele afirma que, “[...] dependendo da escala geográfica em que se concentrar nossa observação, estaremos percebendo mais, ora os territórios, ora as redes que os conectam (ou que os compõem)” (Haesbaert, 2006, p. 121-124). Essa formulação permite compreender que o *LPR* em Pernambuco não vigia o território como um bloco homogêneo, mas como uma rede de pontos de captura ligados por fluxos de informação, bases de dados e rotinas de acionamento.

Isso altera a própria maneira de avaliar a legitimidade territorial do sistema. Se o *LPR* opera como território-rede, não basta perguntar onde há câmeras ou qual é a extensão da cobertura. É preciso perguntar quais nós dessa rede somos privilegiados, que circuitos de circulação recebem atenção reforçada e quais fluxos urbanos passam a ser mais facilmente monitorados, correlacionados e acionados. O próprio Haesbaert (2006, p. 121-124) observa que, no mundo contemporâneo, a rede surge da interação entre múltiplas escalas e territórios, contribuindo para compreender “essas articulações entre diferentes territorialidades bem como suas estruturações internas”, e acrescenta que a sociedade moderna se tornou cada vez mais “reticulada”, marcada por fluxos dinâmicos e pela velocidade crescente dos deslocamentos. A geografia da suspeição, nesse caso, não se mede apenas pela “mancha” da cobertura, mas pela

arquitetura seletiva das conexões. Se a rede de câmeras se concentra sobretudo em eixos que protegem determinados fluxos metropolitanos, logísticos ou socialmente valorizados, ela pode acabar produzindo um território-rede que protege certos circuitos enquanto submete outros a maior rastreabilidade e maior exposição à suspeição.

Esse movimento pode ser lido à luz da noção de “fobópole” (Souza, 2008; Lima, 2014), formulada por Marcelo Lopes de Souza para descrever a cidade atravessada pelo medo generalizado e pela militarização da questão urbana. A utilidade desse conceito, aqui, está em mostrar que a expansão da vigilância não costuma ser apresentada apenas como escolha técnica, mas como resposta natural a um ambiente urbano construído discursivamente como ameaçador. O medo passa a justificar a intensificação permanente da observação, e a cidade deixa de ser vista apenas como espaço de convivência para ser lida também como campo de risco a ser administrado.

Esse ponto é importante porque ajuda a compreender que o crescimento do videomonitoramento não se apoia apenas em promessas de eficiência, mas também em uma racionalidade política do medo. Não por acaso, a instalação de novas câmeras costuma ser comunicada como prova de presença estatal, antecipação de ameaças e fortalecimento da capacidade de resposta. A vigilância aparece, então, como linguagem de governo da insegurança. O problema é que, quando o medo se torna a gramática central da gestão urbana, a exceção tende a se normalizar: mais observação, mais retenção de rastros, mais classificação de passagens e mais naturalização da suspeita passam a ser tratadas como preço normal da proteção (Souza, 2008; Lima, 2014).

É justamente aí que a videovigilância “inteligente” acrescenta uma camada nova. Fernanda Bruno (2012, p. 47-63) observa que esses sistemas “[...] são programados para detecção automatizada e em tempo real de situações consideradas irregulares e/ou suspeitas”. A formulação é decisiva para esta pesquisa porque mostra que o sistema não se limita a registrar a realidade; ele já nasce calibrado para selecionar o que deve aparecer como desvio, risco ou irregularidade. A distribuição territorial da infraestrutura e a lógica de detecção automatizada se reforçam mutuamente: não apenas alguns lugares são mais monitorados, mas neles a atenção da máquina também é moldada para reconhecer certos eventos como mais relevantes do que outros.

Por isso, a legitimidade territorial do *LPR* não pode ser pensada apenas em termos de abrangência ou capacidade de cobertura. Ela depende de saber como se define o mapa da visibilidade estatal. Em uma cidade desigual, tornar certas rotas mais legíveis do que outras é também tornar alguns deslocamentos mais suscetíveis de suspeição. O simples fato de um veículo circular por uma área fortemente capturada pode produzir mais registros, mais correlações e mais chances de acionamento, ainda que isso não corresponda, necessariamente, a um risco substantivo maior. Em outras palavras, a densidade da vigilância interfere na própria produção daquilo que depois aparecerá como ocorrência ou relevância operacional (Bruno, 2012, p. 47-63).

A literatura sobre ordenação social (*social sorting*) ajuda a tornar esse problema mais preciso. Em '*Surveillance as Social Sorting'*, David Lyon (2003) mostra que a vigilância contemporânea depende de bases de dados pesquisáveis e de classificações que distribuem atenção, risco e tratamento diferenciado sobre pessoas e populações. No centro desse processo está a ideia de que a vigilância "[...] obtém dados pessoais e grupais a fim de classificar pessoas e populações de acordo com critérios variados[8]" (*Ibidem*, p. 34). Aplicado ao *LPR*, isso significa que a leitura automática de placas não apenas identifica veículos, mas também participa de uma ordenação social da circulação, na qual certos trajetos se tornam mais monitoráveis, mais facilmente correlacionáveis e, por isso mesmo, potencialmente mais suspeitos do que outros.

Esse efeito é especialmente preocupante em contextos marcados por desigualdade territorial, seletividade racial e diferenças intensas de acesso à cidade. O risco de uma geografia da suspeição não depende de que o sistema tenha sido desenhado para discriminar explicitamente. Basta que ele se estruture sobre critérios de risco territorial, intensidade de fluxo, pontos "sensíveis" e infraestrutura desigual para que certos bairros, rotas ou circuitos de mobilidade passem a concentrar mais vigilância e mais possibilidade de intervenção. O resultado é uma assimetria de legibilidade: algumas partes da cidade aparecem muito mais para o Estado do que outras.

Nesse sentido, a legitimidade territorial exige mais do que publicidade genérica sobre a instalação das câmeras. Ela requer transparência sobre os critérios de

[8] Do original: "[...] obtains personal and group data in order to classify people and populations according to varying criteria".

distribuição dos pontos de captura, revisão periódica de seus efeitos espaciais e mecanismos institucionais capazes de avaliar se a geografia da vigilância está reproduzindo seletividades indevidas. Uma política territorialmente legítima de LPR precisaria, por exemplo, permitir controle público sobre a localização dos PCIs, sobre os padrões de acionamento por área e sobre o impacto da infraestrutura em territórios já tradicionalmente mais policiados. Sem isso, a cidade corre o risco de ser convertida em cartografia automatizada da suspeição.

O ponto central, portanto, é que a legitimidade do sistema começa antes de qualquer alerta individual. Ela começa no modo como o território é transformado em superfície desigual de captação, na forma como o medo legitima a expansão da observação e no modo como a técnica seleciona o que será visto como relevante. Em uma dissertação voltada ao “bom policiamento”, isso significa reconhecer que a distribuição das câmeras não é simples detalhe de implantação. É parte do próprio problema democrático que o *LPR* coloca.

5.3.2 Legitimidade como responsabilidade: controle do genoespaço pelo nomoespaço

A segunda dimensão da legitimidade trabalhada aqui diz respeito à responsabilização e pode ser mais bem compreendida a partir da distinção proposta por Paulo Cesar da Costa Gomes entre nomoespaço e genoespaço. Em ‘A condição urbana’, essa distinção aparece como parte de um esforço mais amplo de pensar o espaço não como pano de fundo neutro da vida social, mas como elemento ativo na organização das relações políticas, jurídicas e simbólicas. O próprio sumário do livro já mostra a centralidade dessa construção teórica, ao dedicar a primeira parte da obra às “duas matrizes territoriais: nomoespaço e genoespaço”, desenvolvidas em capítulos próprios (Gomes, 2020, p. 5). Mais do que nomear dois tipos de espaço, o autor propõe duas matrizes de leitura para compreender como diferentes formas de ordenamento territorial produzem sentidos, vínculos e possibilidades de convivência.

Essa preocupação faz sentido porque, como o próprio Gomes (2002) escreve, “[...] a cidade não pode, pois, ser concebida como uma forma que se produz simplesmente pela contiguidade das moradias ou pelo simples adensamento de população; ela é, antes de qualquer coisa, um tipo de associação entre as pessoas, associação que é uma forma física e um conteúdo” (*Ibidem*, p. 19). Essa passagem é

importante porque mostra que o espaço, para o autor, nunca é apenas materialidade. Ele também carrega regras, imagens, expectativas, valores e formas de relação. É justamente por isso que a distinção entre nomoespaço e genoespaço não deve ser entendida como mera classificação geográfica, mas como forma de perceber diferentes princípios de organização do espaço social.

Em termos mais concretos, o nomoespaço pode ser compreendido como o espaço estruturado pela generalidade da regra, pela possibilidade de convivência entre diferentes sob um mesmo ordenamento e pela presença de princípios impessoais que tornam a vida comum possível. Já o genoespaço remete a uma lógica diferente: ele se aproxima de formas de pertencimento, identidade, proximidade e diferenciação entre “os de dentro” e “os de fora”. Embora a obra não trabalhe essas categorias como opostos absolutamente puros, ela mostra, em vários momentos, a tensão entre um espaço orientado pela abertura à alteridade e outro organizado por marcações identitárias mais fechadas. Isso aparece de forma particularmente nítida quando Gomes (2002, p. 31, 60 e 182) afirma que uma parte da cidade pode ser ocupada por uma dinâmica que funda “[...] uma ideia de território identitário fechado e exclusivo” e acrescenta que “[...] o aumento de territórios identitários significa uma diminuição dos espaços públicos na cidade”.

Transportada para o problema desta dissertação, essa distinção ajuda a tornar mais visível uma tensão central da vigilância algorítmica. Em chave adaptada, pode-se dizer que o genoespaço do *LPR* corresponde à materialidade técnico-operacional do sistema: código, *OCR*, filtros, parâmetros, listas, integrações, bancos de dados e logs. É o plano em que a plataforma lê, classifica, correlaciona e produz visibilidade. Já o nomoespaço, aqui, corresponde ao campo das normas e garantias que deve enquadrar essa infraestrutura: finalidades delimitadas, regras de acesso, critérios de retenção, auditabilidade, possibilidade de revisão, responsabilização e controle externo. A utilidade dessa aproximação está em mostrar que a compatibilidade democrática da vigilância depende de que o espaço das normas consiga efetivamente conter, orientar e revisar o espaço da técnica. Quando a arquitetura do sistema cresce mais rapidamente do que as garantias que deveriam enquadrá-la, abre-se espaço para que a decisão técnica passe a organizar a vigilância com mais força do que a decisão jurídica consegue limitá-la.

Em outras palavras, não basta que a plataforma exista e opere bem. É preciso que sua existência esteja submetida a regras públicas suficientemente claras para

limitar o que ela pode fazer e para tornar visíveis os motivos de cada uso. O problema do *LPR* não está apenas no fato de haver captura automatizada de placas, mas em tudo o que essa captura desencadeia depois, pois quem acessa, quem cruza, quem define parâmetros, quem cria listas de interesse, quem valida alertas e quem responde quando a informação produz uma intervenção indevida. Uma infraestrutura tecnicamente poderosa, se não estiver subordinada a um regime de responsabilidade institucional, tende a ampliar capacidade muito mais rapidamente do que amplia controle.

Essa tensão se aprofunda quando se observa o caráter híbrido do policiamento contemporâneo. Em 'Padrões de policiamento', Bayley (2002, p. 50) lembra que "[...] o policiamento público nunca substitui permanentemente o policiamento privado". A observação é particularmente valiosa para o *LPR* pernambucano porque sua infraestrutura depende de contratação pública, mas também de *softwares*, plataformas, módulos analíticos, *OCR*, integração de sistemas e governança técnica cujos componentes podem ser desenvolvidos, parametrizados ou mantidos por atores privados. O problema, aqui, não é apenas o fato de a segurança pública utilizar serviços tecnológicos contratados; é o risco de que decisões relevantes passem a ser moldadas por lógicas técnicas e administrativas que não atravessam o mesmo escrutínio público exigido da decisão estatal.

A hibridização cria, assim, um problema de imputação. Quando a empresa fornece o módulo, define parâmetros, ajusta filtros ou condiciona as possibilidades de uso, e o Estado opera a plataforma, quem responde por uma classificação errada, por uma seleção indevida ou por um desenho de acesso insuficientemente controlado? É nesse ponto que a diluição da responsabilidade deixa de ser hipótese abstrata e se torna risco concreto. A decisão final pode até permanecer formalmente atribuída ao Estado, mas o enquadramento do que será visível, acionável e prioritário já pode ter sido parcialmente definido por uma arquitetura que opera em zona cinzenta entre o público e o privado (Bayley, 2002).

É por isso que a responsabilização depende diretamente da auditabilidade. No caso pernambucano, o Termo de Referência exige que a plataforma permita "[...] *logs* de acesso e auditoria de todas as ações do usuário" e afirma, em outra seção, que "toda a plataforma deve ser auditável", indicando como um dos principais itens da auditoria os "[...] *logs* de acesso ao sistema e atividade na plataforma", para identificar "quem acessou o sistema" e "realizou determinada ação" (Pernambuco, 2024). Esse

dado é metodologicamente importante porque revela que o próprio desenho da contratação reconhece que a legitimidade do sistema não pode ser dissociada da rastreabilidade de seu uso.

Mas os *logs*, por si, não resolvem o problema. Se o registro se limita a contar consultas, horários e usuários, ele continua operando sobretudo no plano da atividade interna da máquina. Para ter valor democrático real, a auditabilidade precisa permitir reconstruir a cadeia decisória: porque aquele dado foi consultado, em conexão com qual situação concreta, com qual finalidade pública e com qual efeito posterior. Sem isso, os logs se tornam apenas vestígios administrativos do funcionamento do sistema, e não instrumentos capazes de submeter a tecnologia a controle externo efetivo. É nesse sentido que a crítica de Brodeur (2002) à prevalência dos meios sobre os fins ajuda a qualificar a própria ideia de auditabilidade.

Essa exigência se torna ainda mais clara quando se pensa no papel do Ministério Público e de outros órgãos de controle. Em tese, a existência de *logs*, trilhas de auditoria e perfis de acesso abre uma via concreta para o controle externo da atividade policial. Na prática, porém, esse controle só se realiza se houver capacidade institucional para acessar, interpretar e fiscalizar os registros relevantes. Não basta que a plataforma seja “auditável” em abstrato, se os órgãos de controle não dispõem de acesso tempestivo, conhecimento técnico e condições materiais para examinar o funcionamento do sistema. A responsabilização, portanto, não depende apenas da existência dos registros, depende de um arranjo institucional que torne esses registros politicamente úteis.

Daí a importância de pensar a legitimidade também em termos de *accountability*, isto é, de prestação de contas, fiscalização e atribuição clara de responsabilidade pelos usos do sistema, e não apenas como conformidade formal com normas abstratas (Rocha, 2013). No caso do *LPR*, isso significa que não basta a plataforma existir dentro de um contrato ou de uma autorização administrativa, é preciso que seu funcionamento possa ser reconstruído, explicado e controlado. Em chave adaptada, o genoespaço do sistema — seus códigos, *logs*, parâmetros e módulos analíticos — só se torna democraticamente aceitável quando pode ser efetivamente submetido ao nomo-espaço das normas, dos controles e das garantias. Isso exige governança de acesso, regras claras sobre perfis de usuário, critérios de retenção, revisão de listas, auditoria independente e imputação visível de responsabilidade por erros, abusos ou desvios de finalidade. Sem essa subordinação

da técnica ao Direito, a plataforma pode operar com alto desempenho e, ainda assim, permanecer institucionalmente opaca, dificultando justamente aquilo que a *accountability* busca assegurar saber quem decidiu, com base em quê, com qual finalidade e sob qual possibilidade de controle (Poncioni, 2022).

Em síntese, a legitimidade como responsabilização exige que a infraestrutura informacional do policiamento permaneça politicamente atribuível. O ponto decisivo não é apenas saber se o sistema funciona, mas se é possível reconstruir, revisar e contestar o circuito de decisões que vai da captura do dado à intervenção policial. Em matéria de *LPR*, isso significa que o bom policiamento depende menos da inteligência da plataforma do que da capacidade do Estado de governá-la sob critérios públicos e de responder, sem ambiguidade, pelo que ela produz.

5.3.3 Eficácia social como critério de legitimidade democrática

O terceiro eixo que reputamos indispensável à análise do *LPR* é a eficácia social. Aqui, a contribuição de Brodeur (2002) é decisiva porque impede que o sucesso do policiamento seja medido apenas pelos sinais de movimentação interna da organização. Em ‘Como reconhecer um bom policiamento’, ao discutir a avaliação do policiamento orientado para a solução de problemas, Brodeur (2002, p. 72) afirma que o que deve ser medido “[...] acima de qualquer outra coisa é o sucesso das respostas aos problemas previamente identificados e analisados”. A formulação é particularmente útil para o caso pernambucano, porque o videomonitoramento com *LPR* produz com facilidade indicadores de atividade, mas muito menos evidências claras sobre seus efeitos finais.

Essa distinção entre meios e fins é central. Placas lidas, alertas emitidos, incidentes registrados, câmeras instaladas, PCIs implementados, ocorrências abertas e prisões apoiadas pelo sistema são todos indicadores úteis para descrever o funcionamento da infraestrutura. Mas eles ainda pertencem, em grande medida, ao plano dos meios. O que interessa ao “produto externo do policiamento” é outra coisa, é redução de problemas concretos, diminuição de danos, melhora da confiança pública, maior inteligibilidade do uso da força e percepção de justiça no modo como a tecnologia orienta a intervenção estatal.

No caso pernambucano, os materiais públicos divulgados até aqui parecem favorecer muito mais o primeiro plano do que o segundo. A comunicação institucional

destaca a assinatura do contrato para duas mil câmeras, com investimento elevado e integração de inteligência artificial (sds.pe.gov.br, 20214). O Relatório Anual de Ações do Governo, por sua vez, informa 916 pontos de captura e 393 câmeras ativas em 2025 (Pernambuco, 2025). Já a cobertura jornalística baseada em dados da Secretaria de Defesa Social (SDS) aponta que o novo sistema registrou 1.446 incidentes em três meses, média de 16 casos por dia, com 185 ocorrências abertas e 11 prisões (Pernambuco, 2025). Tudo isso mostra operação, expansão e produtividade. O que ainda não demonstra com igual clareza é o impacto final do sistema sobre problemas públicos delimitados.

É exatamente aqui que a crítica de Brodeur (2002, p. 72 e 78) à “síndrome dos meios sobre os fins” se torna mais incisiva, pois, há “um risco genuíno” de que se perpetue essa inversão avaliativa, na qual a atividade institucional passa a valer como prova suficiente de sucesso, mesmo quando o produto final permanece incerto. No caso do *LPR*, esse risco é particularmente forte porque a tecnologia produz números sedutores: a máquina conta tudo, registra tudo, integra tudo, alerta tudo. Mas uma polícia mais capaz de contar não é, por isso, uma polícia melhor.

Essa constatação não significa negar utilidade ao sistema. É perfeitamente plausível que o *LPR* auxilie investigações, localize veículos vinculados a crimes, reconstrua trajetórias e apoie a coordenação policial em tempo quase contínuo. O ponto é que utilidade eventual não se confunde com legitimidade demonstrada. O bom policiamento exige que a tecnologia permaneça subordinada a finalidades delimitadas e avaliáveis, e não que essas finalidades sejam presumidas apenas porque a ferramenta existe, funciona e gera uma estética de modernização administrativa.

A discussão recente sobre eficiência policial no Brasil reforça esse ponto. Rolim e Pereira (2022) mostram que a atividade policial depende da estima e da colaboração do público e que avaliações baseadas apenas em número de prisões, casos resolvidos ou tempo de resposta podem distorcer a percepção da qualidade do policiamento, porque o objetivo central não é acumular processos internos, mas prevenir o crime e aumentar a confiança da população. Esse argumento dialoga diretamente com a crítica de Brodeur (2002), porque medir apenas atividade pode produzir a ilusão de eficácia, quando o que deveria estar em causa é o efeito público da resposta.

É por isso que a eficácia social do *LPR* precisa ser pensada em dois níveis. O primeiro é empírico: o sistema reduziu, de forma verificável, crimes para os quais foi

mobilizado? Houve diminuição de roubos de veículos, melhora do esclarecimento em eventos delimitados, queda da reincidência em certos circuitos, ou redução da vitimização em áreas diretamente associadas ao uso da ferramenta? O segundo nível é democrático: o uso da tecnologia aumentou a confiança da população, tornou a atuação policial mais compreensível e reduziu arbitrariedades, ou apenas expandiu a capacidade de vigilância sem igual demonstração de justiça procedimental? (Poncioni, 2022; Rocha, 2013).

A justiça procedimental é decisiva aqui porque ela desloca a eficácia do plano puramente instrumental para o plano relacional. Uma tecnologia pode ampliar a capacidade de intervenção estatal e, ao mesmo tempo, enfraquecer a legitimidade institucional se operar com baixa transparência, alto grau de opacidade ou seletividade territorial intensa. A população não avalia a polícia apenas pelos números de atividade, mas também pela forma como a autoridade se apresenta, pela possibilidade de contestar decisões e pela percepção de que critérios semelhantes são aplicados de forma justa. É justamente por isso que a literatura brasileira sobre legitimidade policial insiste em *responsiveness* e *accountability* como dimensões estruturantes do policiamento democrático (Poncioni, 2022; Rocha, 2013).

Em ambientes apoiados por IA, esse ponto se torna ainda mais importante. Erros de leitura, falsos positivos, listas desatualizadas, critérios opacos de acionamento e consultas sem justificativa suficiente podem produzir intervenções formalmente amparadas pelo sistema, mas socialmente percebidas como arbitrárias. Se isso acontece, o resultado pode ser paradoxal, uma vez que a tecnologia amplia capacidade operacional ao preço de reduzir confiança pública. Uma infraestrutura mais poderosa, mas menos justificável, não realiza a ideia de bom policiamento; apenas transfere o velho problema da arbitrariedade para uma escala tecnicamente mais sofisticada.

Por isso, uma avaliação democrática do *LPR* não pode ficar satisfeita com indicadores de acionamento. Ela precisa distinguir ocorrências meramente registradas de resultados substantivos, medir o peso de falsos positivos, examinar a distribuição territorial dos alertas, acompanhar o destino das ocorrências abertas e verificar se houve efeito demonstrável sobre o medo e a confiança pública. Sem esse tipo de avaliação, permanece-se muito mais próximo da estética da inovação do que da prova de legitimidade.

Em síntese, a primazia dos fins sobre os meios exige que a vigilância automatizada em Pernambuco seja julgada não pela abundância de seus registros, mas pelo valor público que efetivamente produz. O *LPR* só poderá ser compreendido como compatível com um modelo de legitimidade democrática se demonstrar, ao mesmo tempo, utilidade prática, limites jurídicos, controlabilidade institucional e efeitos socialmente relevantes sobre segurança e confiança.

Nessa perspectiva, a legitimidade como eficácia social não se satisfaz com a mera exibição de números de atividade, mas exige publicidade sobre o produto final que o sistema efetivamente entrega. Isso significa que o Estado não deveria apenas divulgar quantas placas foram lidas, quantos alertas foram emitidos ou quantas câmeras foram instaladas, mas demonstrar, de forma verificável, se o *LPR* contribuiu para reduzir crimes específicos que justificaram sua adoção, como o roubo de veículos, e em que medida essa contribuição ocorreu. A crítica de Brodeur (2002) ajuda precisamente a sustentar esse deslocamento, porque ela mostra que o problema do bom policiamento não está em multiplicar meios, mas em comprovar o valor público das respostas produzidas. Sem essa exigência de demonstração pública do resultado, o sistema corre o risco de se converter em algo institucionalmente vistoso, tecnicamente sofisticado e politicamente rentável, mas ainda assim incapaz de provar que produz segurança em sentido relevante. E é precisamente para impedir essa inversão que a crítica de Brodeur (2002) continua tão importante para este trabalho. Nesse caso, o videomonitoramento apoiado por *LPR* deixaria de ser instrumento de bom policiamento para se aproximar de um exercício caro de estética de modernização administrativa.

6 CONSIDERAÇÕES FINAIS

No início desta dissertação, prevalecia uma compreensão predominantemente favorável acerca do videomonitoramento inteligente com leitura automática de placas em Pernambuco. Em um primeiro momento, essa tecnologia se apresentava como instrumento particularmente relevante para a atuação policial, na medida em que ampliaria a capacidade de localização de veículos, subsidiaria investigações e contribuiria para maior eficiência da resposta estatal em contextos de risco. Sob tal perspectiva inicial, o *LPR* parecia configurar um desdobramento quase evidente do aperfeiçoamento das políticas de segurança pública.

Entretanto, ao longo do desenvolvimento da pesquisa, essa compreensão foi progressivamente reformulada. O aprofundamento da discussão teórica, a análise do marco jurídico aplicável e a reconstrução documental do caso pernambucano evidenciaram que a implementação dessa tecnologia não se esgota em seus potenciais benefícios operacionais. Ao contrário, sua adoção também suscita questões substantivas relativas à legitimidade, aos mecanismos de controle, à seletividade de sua incidência e às exigências de justificação pública, as quais não podem ser relegadas à condição de efeitos marginais ou secundários.

Essa mudança de perspectiva foi, em si, um dos resultados mais importantes alcançados ao longo da escrita. A reflexão partiu de uma inquietação concreta sobre o uso do *LPR* em Pernambuco, mas logo demonstrou que esse fenômeno não pode ser lido como simples modernização técnica. O que está em jogo é um deslocamento mais profundo na forma de observar, registrar e governar a cidade. As teorias discutidas nos capítulos iniciais permitiram mostrar que o videomonitoramento apoiado por inteligência artificial se insere em um movimento mais amplo de transformação da vigilância contemporânea, no qual o foco deixa de estar apenas na observação pontual e se desloca para a produção contínua de rastros, padrões e inferências. O problema central, assim, não era apenas saber se a tecnologia funciona, mas em que medida seu uso é compatível com critérios democráticos de legitimidade e com a ideia de bom policiamento.

Os capítulos teóricos evidenciaram que esse deslocamento pode ser compreendido a partir de uma dupla chave. De um lado, a tradição do panoptismo, em Bentham e Foucault, ajuda a entender a centralidade da visibilidade como técnica de governo. De outro, as leituras da sociedade de controle e da vigilância

contemporânea permitiram perceber que, no ambiente digital, essa visibilidade já não depende apenas da presença humana ou do olhar fixo sobre um espaço delimitado. Ela passa a operar por meio da coleta, indexação, cruzamento e acionamento de dados em tempo quase contínuo. Nesse quadro, o *LPR* se revelou particularmente importante porque transforma o movimento efêmero do cidadão em rastro consultável e indexável, alterando o próprio estatuto do espaço público. O que antes podia desaparecer no fluxo ordinário da circulação passa a se converter em evento recuperável, correlacionável e potencialmente acionável pela máquina estatal.

Essa conclusão foi reforçada quando a análise se voltou ao caso pernambucano. A reconstrução documental da infraestrutura mostrou que o sistema não se resume à presença física de câmeras espalhadas pela cidade. O videomonitoramento inteligente com *LPR* aparece, na realidade, como uma cadeia sociotécnica composta por pontos de captura, centros de gerenciamento, plataformas de *VMS*, módulos de leitura automática, regras de acesso, registros de auditoria e processos de integração entre imagem, dado, alerta e decisão. Em vez de simples registro visual, o sistema cria uma verdadeira escrita sobre o movimento. A circulação é convertida em dado estruturado, o dado, em consulta, a consulta, em alerta, e o alerta, em possibilidade de ação policial. Com isso, a legitimidade do sistema não pode ser reduzida à autorização formal para instalar câmeras. Ela depende da transparência sobre como a imagem é transformada em informação e, mais adiante, em critério de decisão operacional.

A observação do caso pernambucano também revelou que a expansão do sistema vem sendo publicamente apresentada em chave de modernização e eficiência. A instalação de novos pontos de captura, a contratação de infraestrutura integrada e a divulgação de incidentes e prisões associadas ao sistema mostram que a tecnologia já ocupa lugar relevante no discurso institucional da segurança pública. Ao mesmo tempo, porém, os materiais públicos analisados demonstram mais claramente a expansão da capacidade operacional do que os seus efeitos finais em sentido democrático. Em outras palavras, o Estado já conseguiu tornar visível que o sistema funciona e produz atividade; ainda não demonstrou com a mesma clareza que ele produz, de forma verificável, resultados públicos proporcionais, controláveis e socialmente justificáveis.

No plano jurídico, a análise evidenciou uma tensão estrutural entre a expansão prática dessas tecnologias e a capacidade normativa de acompanhá-las com

salvaguardas adequadas. A LGPD reafirma a centralidade da proteção de dados como tema de direitos, mas a exclusão de tratamentos para segurança pública e investigação penal cria um espaço de exceção que, na prática, tende a fragilizar a transparência e a contestabilidade justamente onde o Estado opera com maior poder. Isso não significa negar a importância da segurança pública, mas reconhecer que a ausência de um marco específico robusto pode permitir que sistemas altamente intrusivos se consolidem com governança insuficiente, deslocando o equilíbrio entre eficiência operacional e proteção de direitos.

Foi justamente para responder a essa insuficiência que o capítulo 5 assumiu papel decisivo na parte final do texto. Sua reformulação permitiu abandonar uma abordagem mais genérica sobre legitimidade e construir uma síntese normativa propriamente voltada ao caso pernambucano. A contribuição central passou, então, a consistir na proposição de um modelo analítico de legitimidade democrática da vigilância, estruturado em três eixos, quais sejam: territorial, de responsabilização e de eficácia social. Essas dimensões não foram tratadas como um esquema pronto retirado de uma única obra, mas como sistematização construída a partir do diálogo entre a literatura sobre vigilância contemporânea, o referencial de bom policiamento, os debates sobre policiamento democrático e a reconstrução documental da implantação do *LPR* em Pernambuco.

No eixo territorial, a conclusão foi a de que o *LPR* institui em Pernambuco um verdadeiro território-rede de vigilância. A distribuição dos pontos de captura, a concentração em determinados eixos estratégicos e a capacidade de transformar fluxos urbanos em dados pesquisáveis mostram que a tecnologia não se projeta sobre um território homogêneo, mas sobre circuitos, conexões e nós privilegiados. A leitura feita a partir de Haesbaert, Marcelo Lopes de Souza, Fernanda Bruno e David Lyon permitiu sustentar que a legitimidade territorial do sistema depende de critérios públicos e equitativos de instalação e operação. Sem isso, a rede de vigilância tende a reforçar geografias da suspeição, tornar alguns espaços mais legíveis e mais suspeitáveis do que outros e aprofundar a lógica da fobópole, em que o medo urbano legitima a normalização da observação contínua.

No eixo da responsabilização, ficou demonstrado que a legitimidade do sistema depende de algo mais exigente do que a mera existência de contrato, base tecnológica ou autorização administrativa. A vigilância algorítmica envolve uma cadeia sociotécnica composta por plataforma, regras de acesso, parâmetros, filtros, *logs*,

operadores, gestores e instâncias de decisão. Em um sistema assim, a pergunta “quem responde?” não é trivial. A investigação permitiu concluir que, sem auditabilidade efetiva, rastreabilidade dos usos, governança clara dos acessos e possibilidade de controle externo, a responsabilidade tende a se diluir entre máquina, operador, contratada e administração pública. A tecnologia pode funcionar com alto desempenho e, ainda assim, permanecer institucionalmente opaca. Nessa chave, o argumento desenvolvido sustentou que a legitimidade depende de que a infraestrutura técnica seja efetivamente subordinada às normas, às garantias e aos mecanismos de prestação de contas.

No eixo da eficácia social, a crítica de Jean-Paul Brodeur ofereceu o critério decisivo para o juízo normativo formulado ao final da análise. A conclusão foi a de que o *LPR* só pode ser considerado compatível com o bom policiamento se for capaz de demonstrar seu produto final, e, não apenas exibir a intensidade de sua atividade interna. Isso significa que placas lidas, câmeras instaladas, alertas emitidos e incidentes registrados são dados relevantes, mas insuficientes. Eles pertencem sobretudo ao plano dos meios. A legitimidade, por sua vez, exige demonstração pública de redução de problemas concretos, como roubos de veículos, melhoria verificável do trabalho policial, redução de arbitrariedades e aumento da confiança pública. Sem isso, a tecnologia corre o risco de produzir apenas uma estética de modernização administrativa vistosa, sofisticada, politicamente rentável, mas insuficientemente provada em seu valor público.

É também nesse ponto que a noção de bom policiamento se mostra mais fecunda como horizonte normativo do estudo. Ao longo da análise, tornou-se claro que essa ideia não deve ser confundida com produtividade bruta, expansão da capacidade de vigilância ou simples sofisticação tecnológica. Seu valor está justamente em funcionar como critério para distinguir um policiamento apenas eficiente de um policiamento efetivamente legítimo. Em vez de tomar a tecnologia como prova suficiente de aperfeiçoamento institucional, a ideia de bom policiamento obriga a perguntar se a ação estatal permanece limitada por regras públicas, se é controlável, se seus efeitos são justificáveis e se sua atuação pode ser compreendida como compatível com um ideal democrático de autoridade. Nesse sentido, o conceito de um policiamento ideal não aparece aqui como descrição de uma realidade pronta, mas como horizonte crítico, visto que orienta uma forma de atuação que combina

capacidade operacional com legalidade, responsabilidade, contenção do poder e resposta pública justificável.

É justamente nesse ponto que a análise responde, de forma mais direta, ao seu problema inicial. O uso do *LPR* em Pernambuco não pode ser considerado, no estado atual do exame desenvolvido, automaticamente incompatível com a legitimidade democrática, mas também não pode ser tomado como legitimado apenas por existir, funcionar e produzir números. A conclusão a que se chega é mais exigente: sua compatibilidade democrática permanece condicionada à existência de governança institucional capaz de limitar o poder estatal, submeter a infraestrutura técnica ao controle público e demonstrar resultados socialmente relevantes. O *LPR* não melhora nem piora o policiamento em Pernambuco de forma intrínseca. O que define sua legitimidade é a forma como ele é governado, limitado, fiscalizado e justificado perante a coletividade.

Também foi necessário reconhecer as limitações da análise realizada. Por se tratar de uma investigação qualitativa baseada predominantemente em bibliografia e análise documental, o estudo utilizou essencialmente fontes públicas, como: editais, termos de referência, relatórios, materiais institucionais e cobertura jornalística. Essa opção foi metodologicamente adequada ao objetivo de reconstruir a cadeia formal de implantação do sistema e os critérios públicos de sua justificação. No entanto, ela impõe limites importantes. Não houve acesso a *logs* operacionais reais, registros completos de auditoria, protocolos internos de uso cotidiano, listas efetivamente empregadas, bases analíticas do sistema nem observação direta da cadeia de decisão policial em campo. Tampouco foram realizadas entrevistas com operadores, gestores, integrantes do Ministério Público, defensores públicos ou cidadãos diretamente afetados por abordagens apoiadas por IA. Isso significa que parte das conclusões teve de se concentrar no que o próprio poder público escolheu tornar visível, e não no funcionamento integral e empiricamente observável da plataforma.

Essas limitações, longe de reduzir a importância do tema, indicam caminhos fecundos para seu amadurecimento. Seria especialmente valioso, em pesquisas futuras, realizar estudos empíricos sobre o uso cotidiano do sistema, a governança concreta dos acessos, o papel efetivo dos logs e a capacidade real de fiscalização por órgãos de controle. Também seria importante aprofundar a análise dos vieses territoriais em Pernambuco, com métodos georreferenciados capazes de demonstrar

como a distribuição dos pontos de captura e dos alertas afeta diferentes áreas da cidade e da região metropolitana.

Outro caminho promissor diz respeito à justiça procedimental, pois é preciso investigar como o cidadão percebe abordagens ou intervenções apoiadas por IA, se as considera mais seguras, mais neutras ou mais arbitrárias, e em que medida isso afeta a confiança pública na polícia. Além disso, a própria maturação normativa do tema recomenda novas investigações sobre o diálogo entre proteção de dados, prova penal, segurança pública e regulação de sistemas algorítmicos.

Ao final do percurso, consolidou-se uma convicção que não estava dada em seu início. O debate sobre videomonitoramento inteligente com leitura automática de placas não pode ser reduzido à contraposição simplista entre eficiência e direitos, nem à crença de que toda inovação tecnológica traz, por si, ganho de legitimidade. O desafio está em construir formas de uso estatal da tecnologia que não transformem a cidade em espaço de suspeição permanente e que não tratem os direitos fundamentais como meros obstáculos operacionais. Se este texto tem alguma contribuição própria, ela talvez resida justamente em mostrar que a compatibilidade democrática do *LPR* em Pernambuco é um resultado institucional, e não uma qualidade natural da ferramenta. Em última análise, a tecnologia não melhora nem piora o policiamento de forma intrínseca; sua compatibilidade democrática é resultado direto da capacidade de governança institucional de limitar o poder estatal, de submeter o rastro digital ao controle público e de manter a vigilância sob exigências de justificabilidade democrática.

REFERÊNCIAS

A3A ENGENHARIA. **Sistema de Gerenciamento de Vídeo (VMS)**. 2025. Disponível em: https://a3aengenharia.com.br/conteudo/artigos-tecnicos/sistema-de-gerenciamento-de-video/. Acesso em: 17 dez. 2025.

AGAMBEN, Giorgio. **Estado de exceção**. Tradução Iraci D. Poleti. São Paulo: Boitempo, 2004.

AGUILAR, Carolina Bracco Delgado de; DUQUE DE PINHO, Carolina Moutinho. A datificação das cidades na era informacional: o processo de grilagem digital. *In:* Encontros Nacionais da Associação Nacional de Pós-Graduação e Pesquisa em Planejamento Urbano e Regional (ENAMPUR), 20, 2023, Belém. **Anais** [...]. Belém: ANPUR, 2023. Disponível em: https://anpur.org.br/wp-content/uploads/2023/05/st07-02.pdf. Acesso em: 6 jun. 2025.

ALBINO, João Pedro; VALENTE, Vânia (Orgs.). **Inteligência artificial e suas aplicações interdisciplinares**. Curitiba: CRV, 2023.

ALMEIDA, Eduarda Costa. Os grandes irmãos: o uso de tecnologias de reconhecimento facial para persecução penal. **Revista Brasileira de Segurança Pública,** São Paulo, v. 16, n. 2, p. 264–283, fev./mar. 2022. Disponível em: https://revista.forumseguranca.org.br/rbsp/article/view/1377. Acesso em: 6 jun. 2025.

ARISTÓTELES. **Organon:** analíticos posteriores. Tradução Edson Bini. São Paulo: Loyola, 2005.

AZEVEDO, Ana Luísa Vieira de; RICCIO, Vicente; RUEDIGER, Marco Aurélio. A utilização das estatísticas criminais no planejamento da ação policial: cultura e contexto organizacional como elementos centrais à sua compreensão. **Ciência da Informação**, Brasília, v. 40, n. 1, p. 9-21, 2011. Disponível em: https://www.scielo.br/j/ci/a/VrGbrXwwf3V7GBxC9FBWqpQ/. Acesso em: 16 mar. 2026.

BORDIGNON, Gabriel Barros. Dispositivos de vigilância como tecnologias de controle no capitalismo de dados: redes sociais e *smart cities*. **Revista de Morfologia Urbana**, v. 8, n. 2, p. e00157, 2020. Disponível em: https://revistademorfologiaurbana.org/index.php/rmu/article/view/157. Acesso em: 13 out. 2025.

BATISTA, Marcela de Moraes. **Muito além da vigilância eletrônica:** um estudo acerca do videomonitoramento em Pernambuco. 2013. 142 f. Dissertação (Mestrado) – Universidade Federal de Pernambuco, Recife, 2013. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/10987/1/DISSERTA%C3%87%C3%83O%20Marcela%20de%20Moraes%20Batista.pdf. Acesso em: 4 maio 2025.

BATISTELLA, João Vitor. **Preditor de *E-mails SPAM***: um *framework* preditivo de alta precisão com *machine learning.* 2025. 24 f. Trabalho de Conclusão de Curso (Graduação) – Bacharelado em Ciência da Computação, Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul, Ibirubá, 2025. Disponível em:

https://repositorio.ifrs.edu.br/bitstream/handle/123456789/2363/1234567892363.pdf. Acesso em: 17 dez. 2025.

BATITUCCI, Eduardo Cerqueira. Gerencialismo, estamentalização e busca por legitimidade: o campo policial militar no Brasil. **Revista Brasileira de Ciências Sociais,** São Paulo, v. 34, n. 101, e3410111, 2019. Disponível em: https://www.scielo.br/j/rbcsoc/a/zdsYrxddhTwhdTbTJh8dzVH/. Acesso em: 16 mar. 2026.

BAYLEY, David H. **Padrões de policiamento:** uma análise comparativa internacional. 2. ed. São Paulo: EDUSP, 2002.

BECKER, Howard. **Outsiders:** estudos de sociologia do desvio. Tradução Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2008. Disponível em: https://www.leme.uerj.br/wp-content/uploads/2010/10/becker-howard-s-outsiders-estudos-de-sociologia-do-desvio.pdf. Acesso em: 10 abr. 2025.

BENTHAM, Jeremy. **O Panóptico**. Organização Tomaz Tadeu. Traduções de Guacira Lopes Louro, M. D. Magno e Tomaz Tadeu. 2. ed. Belo Horizonte: Autêntica, 2008. Disponível em: https://fauufpa.org/wp-content/uploads/2018/05/tc-o-panc3b3ptico.pdf. Acesso em: 1 abr. 2026.

BERNARDI, Ely. **Sistemas de reconhecimento automático de placas veiculares:** modelo sistêmico e falhas na operação. Tese (Doutorado) – Universidade de São Paulo, São Paulo, 2016. Disponível em: https://www.teses.usp.br/teses/disponiveis/3/3138/tde-11052016-162646/publico/PPGET_Corrigida_2015_ElyBernardi.pdf. Acesso em: 15 dez. 2025.

BIONI, Bruno; GARROTE, Marina; GUEDES, Paula. **Temas centrais na regulação de IA:** o local, o regional e o global na busca da interoperabilidade regulatória. São Paulo: Associação *Data Privacy* Brasil de Pesquisa, 2023. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2023/12/dataprivacy_nota-tecnica-temas-regulatorios.pdf. Acesso em: 10 fev. 2026.

BOOLE, George. **An investigation of the laws of thought on which are founded the mathematical theories of logic and probabilities**. New York: Dover Publications, 1958.

BORDIGNON, Gabriel Barros. Dispositivos de vigilância como tecnologias de controle no capitalismo de dados: redes sociais e *smart cities*. **Revista de Morfologia Urbana,** Rio de Janeiro, v. 8, n. 2, p. e00157, 2020. Disponível em: https://revistademorfologiaurbana.org/index.php/rmu/article/view/157. Acesso em: 13 out. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Nota Técnica nº 29, de 2024**. Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nota-tecnica-29_2024.pdf. Acesso em: 13 fev. 2026.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil, de 5 de outubro de 1988**. Brasília, DF: Congresso Nacional, [2026]. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 12 set. 2025.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 6 out. 2025.

BRASIL. **Medida Provisória n.º 869, de 27 de dezembro de 2018**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Brasília, DF: Presidência da República, [2018]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/mpv/mpv869.htm. Acesso em: 6 out. 2025.

BRICALLI, Iafet Leonardi. A vigilância como cultura. **Sociologia & Antropologia**, Rio de Janeiro, v. 10, n. 3, p. 1.103-1.107, 2020. Disponível em: https://www.scielo.br/j/sant/a/VLq7t8vB4dzcnR7C9MNkW9h/. Acesso em: 12 set. 2025.

BRICALLI, Iafet Leonardi. **O paradoxo da cidade monitorada:** vigilância limitada e espaços públicos fragilizados a partir do estudo do sistema das câmeras do município de Vila Velha – ES. 2015. 183 f. Dissertação (Mestrado em Geografia) – Programa de Pós-Graduação em Geografia, Universidade Federal do Espírito Santo, Vitória, 2015. Disponível em: https://ape.es.gov.br/Media/ape/PDF/Disserta%C3%A7%C3%B5es%20e%20Teses/Geografia/UFES_PPGG_IAFET_LEONARDI_BRICALLI.pdf. Acesso em: 10 fev. 2026.

BRODEUR, Jean-Paul. Policiamento ‘sob medida’: um estudo conceitual. *In:* BRODEUR, Jean-Paul (Org.). **Como reconhecer um bom policiamento:** problemas e temas. São Paulo: EDUSP, 2002.

BRUNO, Fernanda. Contramanual para câmeras inteligentes: vigilância, tecnologia e percepção. **Galáxia**, São Paulo, n. 24, p. 47-63, 2012. Disponível em: https://revistas.pucsp.br/index.php/galaxia/article/view/9807. Acesso em: 13 out. 2025.

BRUNO, Fernanda. **Máquinas de ver, modos de ser:** vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013.

BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2018.

BRUNO, Fernanda. Máquinas de ver, modos de ser: visibilidade e subjetividade nas novas tecnologias de informação e de comunicação. **Revista FAMECOS**, Porto Alegre, v. 11, n. 22, p. 18-51, 2004. Disponível em:

https://revistaseletronicas.pucrs.br/ojs/index.php/revistafamecos/article/view/3271. Acesso em: 8 ago. 2025.

BRUNO, Fernanda. Rastrear, classificar, performar. **Ciência e Cultura**, São Paulo, v. 68, n. 1, p. 61-65, 2016. Disponível em: https://cienciaecultura.bvs.br/scielo.php?pid=S0009-67252016000100012&script=sci_arttext. Acesso em: 15 dez. 2025.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: intersectional accuracy disparities in commercial gender classification. **Proceedings of Machine Learning Research**, v. 81, p. 1-15, 2018. Disponível em: https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Acesso em: 10 dez. 2025.

CANADÁ. **Innovation, science and economic development Canada.** The artificial intelligence and data act (AIDA): companion document. Ottawa: Government of Canada, 2023. Disponível em: https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document. Acesso em: 8 jul. 2025.

CANADIAN HUMAN RIGHTS COMMISSION. **Facial recognition technology use in policing**. Ottawa: Canadian Human Rights Commission, 2022. Disponível em: https://www.chrc-ccdp.gc.ca/about-human-rights/publications/facial-recognition-technology-use-policing. Acesso em: 8 jun. 2025.

CANDIOTTO, César. Disciplina e segurança em Michel Foucault: a normalização e a regulação da delinquência. **Psicologia & Sociedade,** [s.l.], v. 24, número especial, p. 18-24, 2012. Disponível em: https://www.scielo.br/j/psoc/a/gwdGTsHtp4hxNGyLhQybKcs/. Acesso em: 8 ago. 2025.

CLARK, Brian; WHITAKER, Matthew. Municipal Bans on Facial Recognition Technology in the United States. **Journal of Law & Technology**, [s.l.], v. 35, 2023.

COMISSÃO de Administração aprova recursos para Secretaria da Copa. **ALEPE**, 11 abr. 2012. Disponível em: https://www.alepe.pe.gov.br/2012/04/11/comissao-de-administracao-aprova-recursos-para-secretaria-da-copa/. Acesso em: 4 jun. 2025.

COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS (CNPD). **Videovigilância**. Lisboa: CNPD, [s.d.]. Disponível em: https://www.cnpd.pt/organizacoes/areas-tematicas/videovigilancia/. Acesso em: 15 fev. 2026.

CONGRESSO NACIONAL. **Relatório Final dos trabalhos da Comissão de Juristas responsável pela revisão e atualização do Código Civil**. Brasília, DF: CN, [s.d.]. Disponível em: file:///C:/Users/anago/Downloads/ARQUIVO_PORTAL_CJCODCIVIL_8050ComissaoESPComissaoCJCODCIVIL20240415.pdf. Acesso em: 10 abr. 2026.

CONGRESSO NACIONAL. **Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal (LGPD-Penal)**. Brasília, DF: CN, [2020].

Disponível em: https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf. Acesso em: 15 fev. 2026.

CONGRESSO NACIONAL. Comissão de juristas responsável por subsidiar elaboração de substitutivo sobre inteligência artificial no Brasil. **Relatório final**. Brasília, DF: Senado Federal, [2022]. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento/download/68cc5c01-1f3e-491a-836a-7f376cfb95da. Acesso em: 1 abr. 2026.

CONGRESSO NACIONAL. **Projeto de Lei n.º 2.338, de 2023**. Exposição de Motivos do Projeto de Lei nº 2.338/2023. Brasília, DF: CN, [2023]. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 20 set. 2025.

CONGRESSO NACIONAL. **Projeto de Lei n.º 2.338, de 2023**. Dispõe sobre o uso da inteligência artificial no Brasil. Brasília, DF: CN, [2023]. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 20 ago. 2025.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO (CNMP). **Resolução n.º 279, de 12 de dezembro de 2023**. Dispõe sobre as atribuições do Ministério Público no exercício do controle externo da atividade policial. Brasília, DF: CNMP, [2023]. Disponível em: https://www.cnmp.mp.br/portal/images/CALJ/resolucoes/Resoluo-279-de-2023.pdf. Acesso em: 15 mar. 2026.

CORBANEZI, Elton. Sociedades de controle: a interpretação deleuzeana de Foucault. **Estudos de Sociologia**, Araraquara, v. 23, n. 45, p. 139-154, 2019. Disponível em: https://periodicos.fclar.unesp.br/estudos/article/view/11405. Acesso em: 12 set. 2025.

CORDEIRO, Tiago Samaha. **Reconhecimento automático de placas veiculares:** uma abordagem em visão computacional. 2015. 87 f. Dissertação (Mestrado em Pesquisa Operacional e Inteligência Computacional) - Universidade Candido Mendes, Campos dos Goytacazes, 2015. Disponível em: https://mpoic.ucam-campos.br/wp-content/uploads/2015/11/Tiago-Samaha-Cordeiro1.pdf. Acesso em: 6 fev. 2026.

CORRÊA, Sergio Fernando M.; MACÍAS, Salomón Abasto. O governo das condutas e a constituição da subjetividade: um estudo da sociedade de controle de tipo algorítmica. **Revista de Filosofia Moderna e Contemporânea,** Brasília, v. 8, n. 3, p. 137-153, dez. 2020. Disponível em: https://periodicos.unb.br/index.php/fmc/article/view/34460. Acesso em: 12 set. 2025.

COSTA, Rogério da. Sociedade de controle. **São Paulo em Perspectiva**, São Paulo, v. 18, n. 1, p. 161-167, 2004. Disponível em: https://www.scielo.br/j/spp/a/ZrkVhBTNkzkJr9jVw6TygVC/?lang=pt. Acesso em: 10 set. 2025.

DELEUZE, Gilles. *Post-scriptum* sobre as sociedades de controle. *In:* DELEUZE, Gilles. **Conversações (1972-1990)**. Tradução Peter Pál Pelbart. São Paulo: Editora 34, 1992. Disponível em: https://historiacultural.mpbnet.com.br/pos-modernismo/Post-Scriptum_sobre_as_Sociedades_de_Controle.pdf. Acesso em: 10 set. 2025.

DESCARTES, René. **Meditações metafísicas**. Tradução Bento Prado Júnior. São Paulo: Martins Fontes, 1996.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** fundamentos da lei geral de proteção de dados. 3. ed. São Paulo: Revista dos Tribunais, 2021.

DONEDA, Danilo; MONTEIRO, Laura Schertel Mendes. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. São Paulo: Atlas, 2021.

DUARTE, Daniel Edler; NUNES, Pablo; LIMA, Thallita G. L. **Estudos de vigilância**. Rio de Janeiro: CESeC, 2023. Disponível em: https://nev.prp.usp.br/wp-content/uploads/2023/10/PANOPT_panorama_estudos-vigilancia_FINAL_1707.pdf. Acesso em: 12 set. 2025.

DUARTE, Hendrisy Araujo; OLIVEIRA, Rafael Santos de. O paradoxo da proteção: segurança, direitos fundamentais e o avanço das políticas de reconhecimento facial sem regulação. **Profanações,** [s.l.], v. 12, p. 796-837, 2025. Disponível em https://www.periodicos.unc.br/index.php/prof/article/view/5797. Acesso em: 15 dez. 2025.

EDWARDS, Lilian; VEALE, Michael. Slave to the algorithm? Why a right to an explanation is probably not the remedy you are looking for. **Duke Law & Technology Review**, [s.l.], v. 16, n. 1, p. 18-84, 2017. Disponível em: https://scholarship.law.duke.edu/dltr/vol16/iss1/2/. Acesso em: 15 dez. 2025.

ELESBÃO, Ana Clara Santos. Algoritmos nas sociedades de controle: o papel do controle biopolítico no contexto pandêmico. *In:* Congresso Internacional de Ciências Criminais (PUCRS), 2020, Porto Alegre. **Anais** [...] Porto Alegra: PUCRS, 2020. Disponível em: https://editora.pucrs.br/edipucrs/acessolivre/anais/congresso-internacional-de-ciencias-criminais/assets/edicoes/2020/arquivos/71.pdf. Acesso em: 15 set. 2025.

ENGLAND; WALES. **Court of Appeal**. Bridges, R. (on the application of) *v*. Chief Constable of South Wales Police - EWCA Civ 1058. England and Wales, 2020.

EUROPEAN UNION (EU). **Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)**. Luxembourg: European Parliament, [2024]. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689. Acesso em: 10 fev. 2026.

FERREIRA, Dannielly Leandro de Sousa; NOVAES, Sueli Menelau de; MACEDO, Francisco Guilherme Lima. Cidades inteligentes e inovação: a videovigilância na Segurança Pública de Recife, Brasi. **Cadernos Metrópole**, São Paulo, v. 25, n. 58, p. 1.095-1.122, set/dez 2023. Disponível em: https://www.scielo.br/j/cm/a/BgjpbJwnDqq3wNzVFPsJ8Zz/?lang=pt. Acesso em: 8 jun. 2025.

FERREIRA, Sérgio Rodrigo da Silva. Subjetividade e vigilância algorítmica: notas sobre o agenciamento tecnológico das plataformas de redes sociais. **Revista Psicologia Política,** Manaus, v. 25, p. e23986, 2025. Disponível em: http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1519-549X2025000101403. Acesso em: 13 out. 2025.

FIRMINO, Rodrigo José**.** Securitização, vigilância e territorialização em espaços públicos na cidade neoliberal. **Risco - Revista de Pesquisa em Arquitetura e Urbanismo**, São Paulo, v. 15, n. 1, p. 23-35, 2017. Disponível em: https://revistas.usp.br/risco/article/view/134313. Acesso em: 15 dez. 2025.

FOUCAULT, Michel. **Segurança, território, população**: curso no Collège de France (1977–1978). São Paulo: Martins Fontes, 2008.

FOUCAULT, Michel. **Vigiar e punir:** nascimento da prisão. Tradução Raquel Ramalhete. Petrópolis: Vozes, 1999.

FOUCAULT, Michel. **Vigiar e punir:** nascimento da prisão. 42. ed. Petrópolis: Vozes, 2014.

FOUCAULT, Michel. **Microfísica do poder**. Rio de Janeiro: Graal, 2012.

GARCIA, Rafael de Deus; GONTIJO, Rogério Bontempo Cândido. Algoritmos e segurança pública: controle e vigilância no policiamento baseado em dados. **Revista Latino-Americana de Criminologia**, Brasília, v. 1, n. 1, p. 14-43, 2021. Disponível em: https://periodicos.unb.br/index.php/relac/article/view/36735. Acesso em: 13 fev. 2026.

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

GENEVA CENTRE FOR SECURITY SECTOR GOVERNANCE (DCAF). **The use of video surveillance for police accountability.** Geneva: DCAF, 2021. Disponível em: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_ECA_PP_Video_Surveillance_Paper_FINAL_v20210811_0.pdf. Acesso em: 16 mar. 2026.

GENETEC. **Seu guia completo de videomonitoramento e VMS**. [s. l.], [s.d.]. Disponível em: https://www.genetec.com/br/blog/videomonitoramento-e-vms. Acesso em: 15 dez. 2025.

GOMES, Paulo Cesar da Costa. **A condição urbana**: ensaios de geopolítica da cidade. Rio de Janeiro: Bertrand Brasil, 2002.

GONÇALVES, Daniel S. O panóptico: por uma leitura utilitarista. **Phrónesis – Revista de Ética,** [s.l.], v. 5, n. 1, p. 49–56, 2023. Disponível em: https://periodicos.puc-campinas.edu.br/phronesis/article/view/13736. Acesso em: 10 jul. 2026.

GOVERNO de Pernambuco vai instalar duas mil câmeras de videomonitoramento a partir do primeiro trimestre de 2025. **SDS.PE.GOV.BR**, Notícias, 2024. Disponível em: https://www.sds.pe.gov.br/noticias/12027-governo-de-pernambuco-vai-instalar-duas-mil-cameras-de-videomonitoramento-a-partir-do-primeiro-trimestre-de-2025. Acesso em: 8 jul. 2025.

GRAHAM, Stephen. **Cities under siege:** the new military urbanism. London: Verso, 2010.

HAN, Byung-Chul. **A sociedade da transparência**. Tradução Ênio Paulo Giachini. Petrópolis: Vozes, 2017.

HAESBAERT, Rogério. **Territórios alternativos**. 2. ed. São Paulo: Contexto, 2006.

HARCUP, Tony. **The ethical journalist**. 3. ed. London: Sage, 2021.

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE (IACP). **Automated license plate recognition.** [s. l.], [s. d.]. Disponível em: https://www.theiacp.org/projects/automated-license-plate-recognition. Acesso em: 16 mar. 2026.

JOH, Elizabeth E. The new surveillance discretion: automated suspicion, big data, and policing. **Harvard Law & Policy Review**, Cambridge, v. 10, n. 1, p. 15-42, 2016. Disponível em: https://journals.law.harvard.edu/lpr/wp-content/uploads/sites/89/2016/06/10.1_2_Joh.pdf. Acesso em: 16 mar. 2026.

KRONBAUER, Júlia; OLIVEIRA, Rafael Santos de. Tecnologias de reconhecimento facial e colonialismo de dados no Brasil. **Revista Jurídica Cesumar**, Maringá, v. 24, n. 2, p. 387-398, 2024. Disponível em: https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/12166. Acesso em: 13 out. 2025.

KITCHIN, Rob. **The data revolution**. London: Sage, 2014.

LAZZARETTI, Kellen; SEHNEM, Simone; BENCKE, Fernando Fantoni; MACHADO, Hilka Vier. Cidades inteligentes: *insights* e contribuições das pesquisas brasileiras. **Urbe - Revista Brasileira de Gestão Urbana**, Curitiba, v. 11, p. e20180018, 2019. Disponível em: https://www.scielo.br/j/urbe/a/3LscvBK8vN86Q3fyFvzx7Fw/. Acesso em: 1 abr. 2026.

LEMOS, André; QUEIROZ, Camila; SANTANA, Egideílson; FAGUNDES, Frederico; BALEEIRO, Gabriela. Câmeras de vigilância e cultura da insegurança: percepções sobre as câmeras de vigilância da UFBA. **ALCEU**, Rio de Janeiro, v. 12, n. 23, p. 143-153, 2011. Disponível em: https://revistaalceu-acervo.com.puc-rio.br/media/Artigo11%20Andr%C3%A9%20Lemos%2C%20Camila%20Queiroz%2C

%20Egide%C3%ADlson%20Santana%2C%20Frederico%20Fagundes%20e%20Gabriela%20Baleeiro.pdf. Acesso em: 10 fev. 2026.

LIBERTY; BIG BROTHER WATCH. **Joint briefing on live facial recognition technology in the UK.** London, 2022.

LIMA, Luiz Henrique Mateus. RESENHA: SOUZA, Marcelo Lopes de. Fobópole: o medo generalizado e a militarização da questão urbana. **Revista Eletrônica da Associação dos Geógrafos Brasileiros Seção Três Lagoas**, [s.l.], v. 1, n. 19, p. 104-111, 2014. Disponível em: https://periodicos.ufms.br/index.php/RevAGB/article/view/411. Acesso em: 25 mar. 2026.

LOTT, Yuri Monnerat; CIANCONI, Regina de Barros. Vigilância e privacidade, no contexto do Big Data e dados pessoais: análise da produção da Ciência da Informação no Brasil. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 23, n. 4, p. 117-132, 2018. Disponível em: https://periodicos.ufmg.br/index.php/pci/article/view/22594. Acesso em: 10 set. 2025.

LYON, David. **Surveillance as social sorting:** privacy, risk, and digital discrimination. London; New York: Routledge, 2003. Disponível em: https://infodocks.wordpress.com/wp-content/uploads/2015/01/david_lyon_surveillance_as_social_sorting.pdf. Acesso em: 5 jun. 2025.

LYON, David. **Surveillance studies**: an overview. Cambridge: Polity Press, 2007.

MEDEIROS, João Victor Archegas de; GERALDES, Elen Cristina; SOUSA, Janara; SANTOS, Marcelo Fonseca (Orgs.). **Governança digital:** plataformas de internet, soberania digital e inteligência artificial. Goiânia: UFG, 2023. Disponível em: https://files.cercomp.ufg.br/weby/up/76/o/GOVERNANCA_DIGITAL_plataformas_de_internet__soberania_digital_e_IA_ebook.pdf. Acesso em: 8 jun. 2025.

MELO, Samuel Cerqueira. Implicações do capitalismo de vigilância na constituição do sujeito. **Convergências: Estudos em Humanidades Digitais**, Goiânia, v. 1, n. 6, p. 179-196, 2024. Disponível em: https://periodicos.ifg.edu.br/cehd/article/view/2009/1705. Acesso em: 14 set. 2025.

MELO, Pedro Victor; VISEU, Ana. 20 anos de videovigilância dos espaços públicos em Portugal: panorama e desafios sociopolíticos. **Cadernos de Política Pública**, Lisboa, v. 19, n. 37, p. 1-20, 2024. Disponível em: https://journals.ipl.pt/cpublica/article/download/855/780/3753. Acesso em: 20 mar. 2026.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014.

MUFTI, N.; MUHAMMAD, G.; HUSSAIN, M. *et al*. Automatic number plate recognition: a detailed survey of relevant algorithms. **Sensors**, Basel, v. 21, n. 9, p.

1-45, 2021. Disponível em: https://pmc.ncbi.nlm.nih.gov/articles/PMC8123416/. Acesso em: 17 dez. 2025.

NOVO sistema de câmeras flagra 16 incidentes por dia e resulta em prisões em Pernambuco. **Diário de Pernambuco**, Recife, 26 dez. 2025. Disponível em: https://www.diariodepernambuco.com.br/vida-urbana/2025/12/11703745-novo-sistema-de-cameras-flagra-16-incidentes-por-dia-e-resulta-em-prisoes-em-pernambuco.html. Acesso em: 10 mar. 2026.

NÚCLEO DE ESTUDOS DA VIOLÊNCIA (NEV). **Panorama** – Estudos de Vigilância. São Paulo: USP, 2023. Disponível em: https://nev.prp.usp.br/wp-content/uploads/2023/10/PANOPT_panorama_estudos-vigilancia_FINAL_1707.pdf. Acesso em: 12 set. 2025.

OLIVEIRA, Eduardo Chagas; CARNEIRO, Ivana Libertadoira Borges. Sobre o caráter persuasivo da estrutura panóptica: Bentham, Foucault e as novas tecnologias. **Ideação**, Feira de Santana, n. 33, p. 101-125, 2016. Disponível em: https://periodicos.uefs.br/index.php/revistaideacao/article/view/1284/2744. Acesso em: 8 ago. 2025.

OLIVEIRA, E. C. Bentham, Foucault e as novas tecnologias. **Revista Ideação,** [s.l.], v. 18, n. 2, p. 45-60, 2016.

OLIVEIRA, Antônio. Os policiais podem ser controlados? **Sociologias**, Porto Alegre, a. 12, n. 23, p. 142-175, jan./abr. 2010. Disponível em: https://seer.ufrgs.br/sociologias/article/view/12720. Acesso em: 16 mar. 2026.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). **Recommendation of the council on artificial intelligence**. Paris: OECD, 2019 (Revised in 2024). Disponível em: https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449. Acesso em: 18 ago. 2025.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA (UNESCO). **Recommendation on the ethics of artificial intelligence**. Paris: UNESCO, 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000381137. Acesso em: 1 abr. 2026.

PATRIARCA, Gabriel. Policiamento plural: perspectivas teóricas e agenda de pesquisa. **Dilemas: Revista de Estudos de Conflito e Controle Social**, Rio de Janeiro, v. 16, n. 3, p. e55109, 2023. Disponível em: https://revistas.ufrj.br/index.php/dilemas/article/view/55109. Acesso em: 16 mar. 2026.

PERNAMBUCO. Secretaria de Administração; Secretaria de Defesa Social. **Processo Licitatório n.º 0578.2024.AC-19.PE.0263.SAD.DAG-SDS (Pregão Eletrônico nº 0263.DAG-SDS):** edital e termo de referência para solução integrada de videomonitoramento de vias públicas. Recife: Governo do Estado, [2024]. Disponível em:

https://sistemas.tcepe.tc.br/audinArquivos/licon/processo_licitatorio/edital/988/LICON_Edital_988_2024_578_1417995.pdf. Acesso em: 15 dez. 2025.

PERNAMBUCO. Secretaria de Planejamento, Gestão e Desenvolvimento Regional. **Relatório Anual de Ações do Governo de Pernambuco 2025**. Recife: Governo do Estado, [2025]. Disponível em: https://relatoriodegestao.seplag.pe.gov.br/. Acesso em: 10 mar. 2026.

PERON, André Eduardo dos Reis. Vigilância, controle e novas tecnologias. **Mediações – Revista de Ciências Sociais**, Londrina, v. 23, n. 2, p. 63-83, 2018. Disponível em: https://ojs.uel.br/revistas/uel/index.php/mediacoes/article/download/33884/32220. Acesso em: 10 set. 2025.

PONCIONI, Paula Ferreira. A questão da legitimidade policial na democracia: a educação policial em foco. **Revista Brasileira de Segurança Pública**, São Paulo, v. 16, n. 1, p. 14-29, 2022. Disponível em: https://revista.forumseguranca.org.br/rbsp/article/view/1512. Acesso em: 25 mar. 2026.

PORTUGAL. **Lei n.º 95, de 29 de dezembro de 2021**. Regula a utilização e o acesso a sistemas de videovigilância. Lisboa: Presidência da República, [2021]. Disponível em: https://diariodarepublica.pt/dr/analise-juridica/lei/95-2021-176714548. Acesso em: 15 fev. 2026.

RAFFESTIN, Claude. **Por uma geografia do poder**. São Paulo: Ática, 1993.

RAMOS, João. Controle e vigilância no policiamento baseado em dados: riscos e desafios para a democracia. **Revista de Estudos e Pesquisas sobre as Américas (UnB)**, Brasília, [s.a.]. Disponível em: https://periodicos.unb.br/index.php/relac/article/download/36735/30599/110882. Acesso em: 13 fev. 2026.

RIBEIRO, Iselda Corrêa. Polícia. Tem futuro? Polícia e sociedade em David Bayley. **Sociologias,** Porto Alegre, a. 4, n. 8, p. 444-453, jul./dez. 2002. Disponível em: https://www.scielo.br/j/soc/a/pf8mKJCHV6T8ctfkhPJgMSv/. Acesso em: 16 mar. 2026.

RIBEIRO, Laura Talho. **Tecnologias inteligentes de vigilância:** percepções sobre segurança nos centros urbanos. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro, 2018. Disponível em: https://itsrio.org/wp- Agamben content/uploads/2018/03/laura_talho_smartsurveillance.pdf. Acesso em: 15 out. 2025.

ROCHA, Alexandre Pereira da. Policiamento democrático no Brasil: enquadramentos teóricos e desilusões empíricas. Um estudo das polícias do Distrito Federal. ***Civitas*: Revista de Ciências Sociais,** Porto Alegre, v. 13, n. 1, p. 56-76, 2013. Disponível em: https://revistaseletronicas.pucrs.br/civitas/article/view/14652. Acesso em: 25 mar. 2026.

RODRIGUEZ, Pablo Esteban. Espetáculo do dividual: tecnologias do eu e vigilância distribuída nas redes sociais. **Revista Eco-Pós**, Rio de Janeiro, v. 18, n. 2, p. 57-68, 2015. Disponível em: https://revistaecopos.eco.ufrj.br/eco_pos/article/view/2680. Acesso em: 12 nov. 2025.

RODRIGUES, Ellen Cristina. Sociedade do cansaço e o sujeito do desempenho. **Signos do Consumo,** [s.l.], v. 14, n. 2, p. e196226, 2022. Disponível em: https://revistas.usp.br/signosdoconsumo/article/view/196226. Acesso em: 4 jun. 2025.

ROLIM, Marcos; PEREIRA, Vanessa de Quadros. A eficiência policial e seus indicadores. **Revista Brasileira de Segurança Pública**, São Paulo, v. 16, n. 3, p. 314-331, 2022. Disponível em: https://revista.forumseguranca.org.br/rbsp/article/view/1445. Acesso em: 25 mar. 2026.

ROUVROY, Antoinette; BERNS, Thomas. Governamentalidade algorítmica e perspectivas de emancipação: o díspar como condição de individuação pela relação? **Revista ECO PÓS**, [s.l.], v. 18, n. 2, p. 36-56, 2015. Disponível em: https://dipot.ulb.ac.be/dspace/bitstream/2013/225663/3/Governamentalidade_algoritmica.pdf. Acesso em: 6 fev. 2026.

RUSSELL, Stuart. **Inteligência artificial a nosso favor:** porque o futuro da humanidade depende de como lidamos com as máquinas. Tradução Alexandre Martins. Rio de Janeiro: Intrínseca, 2021.

RUSSELL, Stuart; NORVIG, Peter. **Inteligência artificial:** um enfoque moderno. Madrid: Pearson, 2004.

SANTOS, Rômulo Ballestê Marques dos; PORTUGAL, Francisco Teixeira. O panóptico e a economia visual moderna: do panoptismo ao paradigma panóptico na obra de Michel Foucault. **Revista Psicologia Política**, [s.l.], v. 19, n. 44, p. 34-49, jan./abr. 2019. Disponível em: https://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1519-549X2019000100006. Acesso em: 8 ago. 2025.

SDS cria projeto para instalar câmeras de reconhecimento de criminosos e veículos roubados. **Diário de Pernambuco,** Recife, 18 set. 2020. Disponível em: https://www.diariodepernambuco.com.br/noticia/vidaurbana/2020/09/sds-cria-projeto-para-instalar-cameras-de-reconhecimento-de-criminosos.html. Acesso em: 15 ago. 2025.

SEARLE, John R. Minds, brains and programs. **Behavioral and Brain Sciences**, Cambridge, v. 3, n. 3, p. 417-457, 1980.

SILVA, Alessandro Siqueira e; SILVA, Karina Flamino Lugarini; LORENÇÃO, Pâmela Soares; BARROS, Sérgio da Silva. **Estudo de Vulnerabilidades em Sistemas de Videomonitoramento**. 2020. 52 f. Trabalho de Conclusão de Curso (Graduação em Segurança da Informação) – Faculdade de Tecnologia de São Caetano do Sul, São Caetano do Sul, 2020. Disponível em:

https://ric.cps.sp.gov.br/bitstream/123456789/5261/1/02_Kleber_20200630.pdf. Acesso em: 16 dez. 2025.

SILVA, Tarcízio. Visão computacional e racismo algorítmico: branquitude e opacidade no aprendizado de máquina. **Revista da Associação Brasileira de Pesquisadores/as Negros/as,** [s.l.], v. 12, n. 32, p. 335-357, 2020. Disponível em: https://abpn.emnuvens.com.br/site/article/download/744/774. Acesso em: 4 jun. 2025.

SILVA, Adriano Teles da; PEREIRA, Jaks Daienne Galvão; LIMA FILHO, João Rodrigues; BOSNICH, Sérgio Luiz. Policiamento orientado pela inteligência: importância e iniciativas no cenário brasileiro. **Revista Ciência & Polícia**, Brasília, v. 6, n. 2, p. 104-130, 2021. Disponível em: https://revista.iscp.edu.br/index.php/rcp/article/view/291. Acesso em: 16 mar. 2026.

SIQUEIRA, Dirceu Pereira. Autodeterminação informativa na sociedade pós-panóptico. **Prisma Jurídico**, São Paulo, v. 22, n. 2, p. 141-165, 2023. Disponível em: https://periodicos.uninove.br/prisma/article/view/20634/10290. Acesso em: 9 ago. 2025.

SOUSA, Noelma Cavalcante de; MENESES, Antonio Basílio Novaes Thomaz de. O poder disciplinar: uma leitura em Vigiar e Punir. **Saberes: Revista Interdisciplinar de Filosofia e Educação**, Natal, v. 1, n. 4, p. 18-35, 2010. Disponível em: https://periodicos.ufrn.br/saberes/article/view/561/510. Acesso em: 10 ago. 2025.

SOUZA, Marcelo Lopes de. **Fobópole:** o medo generalizado e a militarização da questão urbana. Rio de Janeiro: Bertrand Brasil, 2008.

TANG, Junqing; WAN, Li; SCHOOLING, Jennifer; ZHAO, Pengjun; CHEN, Jun; WEI, Shufen. Automatic number plate recognition (ANPR) in smart cities: a systematic review on technological advancements and application cases. **Cities**, [s.l.], v. 129, 2022. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0264275122002724. Acesso em: 17 dez. 2026.

TEIXEIRA, Daniela Pessanha**. Intensidades corporais e subjetividades contemporâneas:** uma reflexão sobre o movimento da *Body Modification*. 2006. 148 f. Dissertação (Mestrado em Psicologia Clínica) – Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2006. Disponível em: https://www.maxwell.vrac.puc-rio.br/9392/9392_1.PDF. Acesso em: 8 ago. 2025.

TEIXEIRA, Fábio Luís S.; CAMINHA, Iraquitan de O.; LIMA NETO, Avelino Aldo de. Duas funções do olhar em Foucault: panoptismo e transoptismo. **Aurora: Revista de Arte, Mídia e Política**, São Paulo, v. 10, n. 29, p. 108-126, 2017. Disponível em: https://revistas.pucsp.br/index.php/aurora/article/view/32335. Acesso em: 9 ago. 2025.

TELES, Edson. Governamentalidade algorítmica e as subjetivações rarefeitas. **Kriterion**, Belo Horizonte, v. 59, n. 140, p. 429-448, 2018. Disponível em:

https://www.scielo.br/j/kr/a/PQTcJnpCGrP7PD5TrXKWzZm/?format=pdf&lang=pt. Acesso em: 15 dez. 2025.

TOSCANO, Stéfano G. R. Notícias da Cloaca Máxima: distância social, dominação e cárcere. *In*: SALES JÚNIOR, Ronaldo *et al*. (Orgs.). **Cárcere e Cidade**. Recife: Instituto Brasileiro Pró-Cidadania, 2012.

TOSTES, Octavio**. A cor do milagre:** o advento da TV em cores no Brasil. 2013. 132 f. Tese (Doutorado em Ciências da Comunicação) – Universidade de São Paulo, São Paulo, 2013. Disponível em: https://teses.usp.br/teses/disponiveis/8/8138/tde-14112013-110528/publico/2013_OctavioTostes_VCorr.pdf. Acesso em: 5 maio 2025.

TRINDADE, Gerson G. O Panóptico (Jeremy Bentham): resenha. **Revista Brasileira de Estudos Políticos**, Belo Horizonte, p. 251-255, 2011. Disponível em: https://pos.direito.ufmg.br/rbep/index.php/rbep/article/view/1407/821. Acesso em: 20 ago. 2025.

TRIGUEIRO, Emilia Suitberta de Oliveira; COSTA, Raul Max Lucas. O empreendedor de si mesmo na sociedade do cansaço: considerações de Jacques Lacan e Byung-Chul Han. *In*: ALMEIDA, Flávio Aparecido de; FERNANDES, Walmir (Orgs.). **Saúde mental:** desafios, perspectivas e análises pós-isolamento social. Guarujá: Editora Científica Digital, 2023. p. 41-57. Disponível em: https://downloads.editoracientifica.com.br/articles/221110764.pdf. Acesso em: 4 jun. 2025.

TURING, Alan M. Computing machinery and intelligence. **Mind,** Oxford, v. 59, n. 236, p. 433-460, 1950. Disponível em: https://courses.cs.umbc.edu/471/papers/turing.pdf. Acesso em: 20 maio 2025.

UNIÃO EUROPEIA (UE). **Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. Estrasburgo: Parlamento Europeu, [2016]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680. Acesso em: 10 fev. 2026.

UNITED STATES OF AMERICA (USA). Government Accountability Office. **Facial recognition technology:** privacy and accuracy issues. Washington, DC: USA, 2021.

VEALE, Michael; ZUIDERVEEN BORGESIUS, Frederik. Demystifying the Draft EU Artificial Intelligence Act: analysing the good, the bad, and the unclear elements of the proposed approach. **Computer Law Review International**, Köln, v. 22, n. 4, p. 97-112, 2021. Disponível em: https://doi.org/10.9785/cri-2021-220402. Acesso em: 10 fev. 2026.

VIANA, Moises dos Santos. A psicopolítica em Byung-Chul Han: introdução para a crítica das novas tecnologias-inovações de poder. **Interseções – Revista de**

Estudos Interdisciplinares, [s.l.], v. 25, n. 2, p. 1-13, 2023. Disponível em: https://www.redalyc.org/journal/412/41277663005/html/. Acesso em: 6 jun. 2025.

WARREN, Ian; LIPPERT, Randy K.; WALBY, Kevin; PALMER, Darren**.** When the profile becomes the population: examining privacy governance and road traffic surveillance in Canada and Australia. **Current Issues in Criminal Justice**, [s.l.], v. 25, n. 2, p. 565-584, 2013. Disponível em: https://dro.deakin.edu.au/articles/journal_contribution/When_the_profile_becomes_the_population_examining_privacy_governance_and_road_traffic_surveillance_in_Canada_and_Australia/20951770. Acesso em: 16 mar. 2026.

WITTGENSTEIN, Ludwig. **Investigações filosóficas**. Tradução José Carlos Bruni. São Paulo: Nova Cultural, 1999.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância:** a luta por um futuro humano na nova fronteira do poder. Tradução George Schlesinger. Rio de Janeiro: Intrínseca, 2020. Disponível em: https://www.intrinseca.com.br/upload/livros/1%C2%BACap-AEraDoCapitalismoDeVigilancia.pdf. Acesso em: 16 out. 2025.

ZUBOFF, Shoshana. **The age of surveillance capitalism**. New York: PublicAffairs, 2019.