



UNIVERSIDADE CHRISTUS

CURSO DE DIREITO

MARIA VITÓRIA SILVA DE OLIVEIRA

**RACISMO E OPACIDADE ALGORÍTMICA NAS TECNOLOGIAS DE
RECONHECIMENTO FACIAL DO ESTADO DO CEARÁ**

FORTALEZA

2026

MARIA VITÓRIA SILVA DE OLIVEIRA

RACISMO E OPACIDADE ALGORÍTMICA NAS TECNOLOGIAS DE
RECONHECIMENTO FACIAL DO ESTADO DO CEARÁ

Trabalho de Conclusão de Curso (TCC)
apresentado ao curso de Direito da
Universidade Christus, como requisito parcial
para obtenção do título de bacharel em Direito.

Orientador: Prof. Me. Rômulo Richard Sales
Matos.

FORTALEZA

2026

Dados Internacionais de Catalogação na Publicação
Centro Universitário Christus - Unichristus
Gerada automaticamente pelo Sistema de Elaboração de Ficha Catalográfica do
Centro Universitário Christus - Unichristus, com dados fornecidos pelo(a) autor(a)

O48r Oliveira, Maria Vitória Silva de.
 Racismo e opacidade algorítmica nas tecnologias de
 reconhecimento facial do estado do Ceará / Maria Vitória Silva de
 Oliveira. - 2026.
 114 f.

 Trabalho de Conclusão de Curso (Graduação) - Centro
 Universitário Christus - Unichristus, Curso de Direito, Fortaleza,
 2026.
 Orientação: Prof. Me. Rômulo Richard Sales Matos.

 1. algoritmo. 2. reconhecimento facial. 3. opacidade. 4. racismo.
 5. vigilância. I. Título.

CDD 340

MARIA VITÓRIA SILVA DE OLIVEIRA

RACISMO E OPACIDADE ALGORÍTMICA NAS TECNOLOGIAS DE
RECONHECIMENTO FACIAL DO ESTADO DO CEARÁ

Trabalho de Conclusão de Curso (TCC)
apresentado ao curso de Direito da
Universidade Christus, como requisito parcial
para obtenção do título de bacharel em Direito.

Orientador: Prof. Me. Rômulo Richard Sales
Matos.

Aprovado em: 03/06/2026

BANCA EXAMINADORA

Prof. Me. Rômulo Richard Sales Matos (Orientador)
Universidade Christus

Prof. Me. Alisson Rodrigo de Araújo Oliveira
Universidade Christus

Prof^a. Ma. Clara Skarlleth Lopes de Araújo Rodrigues
Universidade Christus

À minha avó, Francisca da Silva Pinto, que, mesmo sem acesso à educação formal, abriu caminhos para que eu pudesse realizar este sonho. Que esta conquista também lhe pertença, em reconhecimento a tudo o que representa em minha vida.

AGRADECIMENTOS

Agradeço à minha família e aos meus amigos pela compreensão nos momentos de ausência e pelo incentivo que tornou possível a conclusão desta etapa.

Ao meu pai, Antônio Luiz de Oliveira, agradeço por me ensinar que o conhecimento é a herança mais valiosa que pode ser transmitida.

Ao Carlos Emanuel Doth Lucena, por todos os anos de zelo e afeto dedicados a mim, expresso minha gratidão por ter compartilhado comigo não apenas os momentos de tranquilidade, mas também as inquietações e os medos que acompanharam a construção desta pesquisa. Agradeço por ter sido abrigo, dividindo dificuldades e responsabilidades para que eu pudesse continuar acreditando nos meus objetivos. Muito do que conquistei também carrega a dimensão dos seus esforços e da forma como sempre se dispôs a me ajudar, mesmo quando isso exigia colocar minhas necessidades à frente das suas. Sou grata pela paciência diante das longas horas de silêncio dedicadas à escrita e pelo cuidado presente nos gestos mais simples do cotidiano, que tornaram o peso da caminhada mais suportável nos dias nublados. Obrigada por se alegrar com cada pequena conquista como se fosse sua, por compreender as renúncias que este processo exigiu, por acolher minhas angústias e por nunca permitir que eu atravessasse sozinha os períodos mais difíceis desta jornada.

À Júlia Maia de Meneses Rocha de Souza, por ter transformado minha trajetória acadêmica de maneira tão profunda. Agradeço por ter acreditado em mim desde o primeiro semestre da graduação, abrindo as portas da pesquisa científica e proporcionando experiências decisivas para a minha formação. Sua confiança no meu potencial, muitas vezes maior do que a que eu mesma possuía, foi essencial para que eu permanecesse firme nos períodos mais árduos do curso e mantivesse vivo o encanto pela vida acadêmica. Grande parte do que construí traz, inevitavelmente, a marca dos ensinamentos que me transmitiu ao longo dos últimos cinco anos. Sou grata, ainda, pelo tempo dedicado à leitura deste texto e pelas sugestões que contribuíram para o seu desenvolvimento.

Ao meu orientador, Rômulo Richard Sales Matos, um dos pilares da minha trajetória acadêmica, expresso minha sincera gratidão pela disponibilidade, pela condução atenciosa e pelo compromisso ético demonstrado em cada etapa deste estudo. Agradeço, igualmente, pela gentileza, pela compreensão e pelo respeito com que acolheu minhas inquietações nos momentos mais desafiadores, mesmo diante das inúmeras reformulações,

dúvidas e inseguranças que naturalmente atravessam o processo de escrita. Registro, com especial estima, meu agradecimento pela confiança depositada em minhas ideias, bem como pela autonomia que me foi concedida na feitura desta monografia. Sua orientação foi fundamental para o refinamento das reflexões aqui apresentadas e, sobretudo, para o meu amadurecimento intelectual ao longo de toda a graduação.

Aos membros da banca examinadora, manifesto minha gratidão pelas considerações que certamente contribuirão para o aprimoramento deste trabalho.

RESUMO

O presente trabalho investiga se a opacidade algorítmica, quando associada ao uso de tecnologias de reconhecimento facial na segurança pública, contribui para a perpetuação de discriminações raciais no estado do Ceará. O estudo problematiza a confiança acrítica na suposta neutralidade dos algoritmos, argumentando que a automação de estigmas raciais pode exacerbar a seletividade penal e a criminalização de minorias sociais historicamente marginalizadas. Com o objetivo de perquirir como a falta de transparência reverbera no racismo estrutural, a investigação contextualiza a transição das sociedades disciplinares para regimes de controle datificados, descrevendo o cenário de implementação e funcionamento das tecnologias de identificação facial e examinando os riscos da extração biométrica sem o devido acompanhamento normativo. Trata-se de pesquisa qualitativa, de natureza exploratória e descritiva, fundamentada em levantamento bibliográfico e análise documental sob o método indutivo. O primeiro capítulo examina a passagem das sociedades disciplinares às sociedades de controle, demonstrando como a vigilância contemporânea se articula à circulação contínua de dados, à securitização e ao policiamento preditivo. O segundo capítulo analisa os fundamentos dos algoritmos, da inteligência artificial, dos vieses cognitivos, do racismo algorítmico, da opacidade e da responsabilidade pelas decisões automatizadas. O terceiro capítulo aplica esse arcabouço ao caso cearense, examinando o funcionamento das tecnologias de reconhecimento facial, a infraestrutura estadual de monitoramento, a seletividade penal racializada e os limites jurídicos da Lei Geral de Proteção de Dados Pessoais diante das atividades de segurança pública. Os resultados evidenciam que a infraestrutura de vigilância cearense tende a automatizar classificações discriminatórias já presentes nas práticas policiais, reforçando a associação entre negritude e periculosidade, enquanto a opacidade dos sistemas reduz a capacidade de contestação dos sujeitos atingidos. Conclui-se que a implementação de tecnologias biométricas na segurança pública exige uma agenda regulatória rigorosa, capaz de harmonizar a eficiência tecnológica com os imperativos da igualdade racial e da transparência.

Palavras-chave: algoritmo; reconhecimento facial; opacidade; racismo; vigilância.

ABSTRACT

This research investigates whether algorithmic opacity, when associated with the use of facial recognition technologies in public safety, contributes to the perpetuation of racial discrimination in the state of Ceará. The study challenges uncritical trust in the supposed neutrality of algorithms, arguing that the automation of racial stigmas can exacerbate criminal selectivity and the criminalization of historically marginalized social minorities. With the aim of examining how the lack of transparency reverberates in structural racism, the research contextualizes the transition from disciplinary societies to data-driven control regimes, describing the implementation and operational landscape of facial recognition technologies and examining the risks of biometric data collection without proper regulatory oversight. This is qualitative research, exploratory and descriptive in nature, based on a literature review and documentary analysis using the inductive method. The first chapter examines the shift from disciplinary societies to societies of control, demonstrating how contemporary surveillance is linked to the continuous circulation of data, securitization, and predictive policing. The second chapter analyzes the fundamentals of algorithms, artificial intelligence, cognitive biases, algorithmic racism, opacity, and accountability for automated decisions. The third chapter applies this framework to the case of Ceará, examining the functioning of facial recognition technologies, the state surveillance infrastructure, racialized criminal selectivity, and the legal limits of the Brazilian General Data Protection Law in relation to public security activities. The results show that Ceará's surveillance infrastructure tends to automate discriminatory classifications already present in police practices, reinforcing the association between Blackness and presumed dangerousness, while the opacity of the systems limits the ability of those affected to challenge them. The study concludes that the implementation of biometric technologies in public security requires a rigorous regulatory framework that balances technological efficiency with the imperatives of racial equality and transparency.

Keywords: algorithm; facial recognition; opacity; racism; surveillance.

LISTA DE ABREVIACÕES E SIGLAS

AGEFIS	Agência de Fiscalização de Fortaleza
AMC	Autorquia Municipal de Trânsito e Cidadania
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CERD	Comitê para a Eliminação da Discriminação Racial
CESEC	Centro de Estudos de Segurança e Cidadania
CICC	Centro Integrado de Comando e Controle
CIOPS	Coordenadoria Integrada de Operações de Segurança
CIVFOR	Centro Integrado de Videomonitoramento de Fortaleza
CNJ	Conselho Nacional de Justiça
ETICE	Empresa de Tecnologia do Ceará
ETUFOR	Empresa de Transporte Urbano de Fortaleza
HC	<i>Habeas Corpus</i>
IA	Inteligência Artificial
IFCE	Instituto Federal de Educação, Ciência e Tecnologia do Ceará
LAI	Lei de Acesso à Informação
LAPIN	Laboratório de Políticas Públicas e Internet
LAPISCO	Laboratório de Processamento de Imagem, Sinais e Computação
LEV	Laboratório de Estudos da Violência
LGPD	Lei Geral de Proteção de Dados Pessoais
NESP	Nova Estratégia de Segurança Pública
NIST	<i>National Institute of Standards and Technology</i>
NUVID	Núcleo de Videomonitoramento
ONU	Organização das Nações Unidas
PCA	Portal de Comando Avançado
PCCE	Polícia Civil do Estado do Ceará
PMCE	Polícia Militar do Estado do Ceará
PRF	Polícia Rodoviária Federal
SESEC	Secretaria Municipal da Segurança Cidadã

SESPORTE	Secretaria de Esportes
SME	Secretaria Municipal da Educação
SPIA	Sistema Policial Indicativo de Abordagem
SSPDS-CE	Secretaria da Segurança Pública e Defesa Social do Estado do Ceará
STATUS	Sistema Tecnológico para Acompanhamento de Unidades de Segurança
STJ	Superior Tribunal de Justiça
TJCE	Tribunal de Justiça do Estado do Ceará

SUMÁRIO

1 INTRODUÇÃO	12
2 A ARQUITETURA TECNOLÓGICA DA SOCIEDADE DE CONTROLE	18
2.1 Da sociedade de disciplina... ..	19
2.2 ...à sociedade de controle.....	22
2.3 O uso da tecnologia como instrumento de controle social	26
3 A “CAIXA-PRETA” DO RACISMO: OPACIDADE ALGORÍTMICA, VIESES COGNITIVOS E A REPRODUÇÃO DE HIERARQUIAS RACIAIS.....	35
3.1 Algoritmos: do modelo simples ao aprendizado de máquina.....	36
3.2 Os limites da cognição artificial	39
3.3 Vieses, heurísticas e a transposição de preconceitos ao <i>design</i> tecnológico.....	41
3.4 O racismo algorítmico como um dispositivo tecnológico de racialidade.....	45
3.5 Democracia e opacidade algorítmica: tensões entre a “caixa-preta” e as garantias constitucionais.....	49
3.6 Agência e responsabilidade sobre a decisão automatizada: a centralidade do elemento humano.....	54
4 SELETIVIDADE PENAL E OS LIMITES DA APLICAÇÃO DE TECNOLOGIAS BIOMÉTRICAS NA SEGURANÇA PÚBLICA CEARENSE	58
4.1 Considerações gerais sobre o funcionamento das tecnologias de reconhecimento facial.....	59
4.2 Infraestrutura de vigilância e integração tecnológica na segurança pública do estado do Ceará	62
4.3 Etiquetamento, seletividade penal e racialização do controle no contexto cearense..	69

4.4 LGPD, segurança pública e os limites do reconhecimento facial.....	75
5 CONCLUSÃO.....	83
REFERÊNCIAS	88

1 INTRODUÇÃO

A proliferação de tecnologias algorítmicas no campo da segurança pública tem produzido novas formas de vigilância e controle social. A promessa de incremento na eficiência das políticas de repressão à criminalidade acompanha a difusão desses sistemas, sobretudo em cenários urbanos caracterizados por índices expressivos de violência e pela demanda social por respostas céleres das instituições de segurança.

Nesse contexto, a presente pesquisa aborda a intersecção entre o fenômeno do racismo e a opacidade algorítmica inerente às tecnologias de reconhecimento facial aplicadas na segurança pública. O estudo concentra-se na análise dessas tecnologias no estado do Ceará, notadamente entre os anos de 2022 e 2024, intervalo que compreende a expansão e consolidação do uso de ferramentas biométricas em espaços públicos de grande circulação. O recorte temporal justifica-se, outrossim, por abranger momento posterior à entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD), circunstância que permite examinar mais facilmente os limites da proteção jurídica conferida aos dados biométricos no Brasil. É também um período de maior normalidade informacional e sanitária em relação ao anterior, fortemente afetado pela pandemia de COVID-19. Embora a época indicada constitua o marco principal da investigação, eventos anteriores e posteriores foram considerados quando necessários à compreensão da trajetória tecnológica e normativa que envolve a implementação desses sistemas.

A escolha do Ceará como unidade de análise empírica justifica-se pela convergência entre o crescente investimento em modernização tecnológica e a persistência de assimetrias raciais. O ente federativo tem promovido a expansão de aparatos de videomonitoramento, plataformas inteligentes e tecnologias biométricas, alinhando-se a uma tendência global de informatização das práticas policiais. Ao mesmo tempo, apresenta elevados indicadores de violência, encarceramento e letalidade policial, que incidem com maior prevalência sobre a população negra. Esse cenário torna o caso cearense particularmente relevante para a investigação dos riscos associados ao reconhecimento facial.

A hipótese desta pesquisa fundamenta-se na premissa de que a confiança acrítica na neutralidade algorítmica pode ocultar e, por vezes, naturalizar vieses discriminatórios. Em sociedades marcadas por desigualdades raciais, essa dinâmica adquire maior relevância, uma vez que a automação de estigmas pode intensificar a criminalização de minorias sociais

historicamente marginalizadas. Diante desse quadro, busca-se verificar se as tecnologias de reconhecimento facial empregadas no estado do Ceará têm contribuído para a perpetuação de práticas racistas.

O objetivo geral do trabalho consiste em investigar a possível relação entre opacidade algorítmica e racismo em tecnologias de reconhecimento facial aplicadas à segurança pública. Para alcançar essa finalidade, foram definidos três objetivos específicos. O primeiro dedica-se a contextualizar a vigilância ostensiva a partir do surgimento de uma sociedade de controle, identificando a passagem de formas disciplinares de poder para mecanismos difusos, contínuos e informacionais de monitoramento. O segundo consiste em descrever o funcionamento dos algoritmos e das tecnologias de reconhecimento facial, com atenção à possibilidade de enviesamento dos bancos de dados que alimentam essas ferramentas. O terceiro visa discutir os riscos da opacidade algorítmica sobre a população negra no Ceará, analisando de que modo a ausência de transparência, auditabilidade e contestabilidade pode reforçar padrões de seletividade penal.

Sob o ponto de vista acadêmico, a pesquisa pretende cooperar com os estudos críticos sobre tecnologia e discriminação algorítmica. Ao eleger o Ceará como recorte empírico, o trabalho busca colaborar para o preenchimento de uma lacuna na produção bibliográfica regional, ainda carente de diagnósticos sobre as possíveis implicações das tecnologias de reconhecimento facial em seu território.

A relevância social encontra-se na mobilização de hipóteses a respeito da predominância de perfis negros entre os alvos da repressão penal. O trabalho intenciona compreender se a opacidade algorítmica dificulta a identificação de vieses discriminatórios e limita a capacidade de resposta dos sujeitos atingidos. A partir dessa reflexão, a investigação se propõe a colaborar com a discussão em torno da legitimidade do uso de tecnologias biométricas, avaliando sua eventual serventia na perpetuação de práticas racistas.

No âmbito jurídico, a pesquisa pondera sobre os limites institucionais do uso de tecnologias de reconhecimento facial na segurança pública. Partindo do pressuposto de que a adoção de instrumentos inteligentes ocorre sem o devido acompanhamento normativo, o estudo discute as possíveis implicações da opacidade algorítmica sobre os direitos humanos e fundamentais de determinadas camadas da sociedade cearense.

A investigação adota abordagem qualitativa (Flick, 2008), adequada à análise

interpretativa de fenômenos sociais complexos. Essa opção metodológica permite examinar o reconhecimento facial para além de sua dimensão instrumental, considerando as relações entre tecnologia, poder, Direito e raça. A escolha também se justifica pela natureza do objeto, que envolve documentos, categorias teóricas, dados institucionais e problemas normativos cuja compreensão exige uma hermenêutica sensível às nuances sociais, políticas e jurídicas da sociedade cearense.

Ademais, a pesquisa possui natureza exploratória e descritiva (Gil, 2022). A dimensão exploratória decorre do caráter ainda incipiente dos estudos jurídicos regionais sobre reconhecimento facial, racismo algorítmico e opacidade no contexto cearense. O trabalho busca, então, ampliar a familiaridade com o tema, organizar referenciais teóricos e identificar categorias analíticas capazes de sustentar futuras investigações.

A vertente descritiva, por sua vez, manifesta-se no exame dos contornos assumidos pela implementação das tecnologias de reconhecimento facial no Ceará, com atenção ao funcionamento dos sistemas biométricos, à infraestrutura de vigilância, aos discursos institucionais, às dinâmicas de opacidade e aos riscos associados ao uso desses instrumentos na segurança pública.

O delineamento metodológico corresponde a um estudo de caso (Gil, 2022). A opção por esse procedimento decorre da necessidade de perquirir a inserção concreta da tecnologia em uma estrutura de dominação específica. Nessa perspectiva, o estudo de caso permite examinar de forma situada a articulação entre modernização tecnológica e seletividade racial em um estado atravessado por assimetrias de poder.

O método utilizado é o indutivo (Lakatos, 2021). A pesquisa parte da observação do caso concreto cearense para construir uma compreensão mais ampla sobre a conexão entre racismo, opacidade algorítmica e vigilância biométrica. Esse percurso foi estruturado em duas etapas principais: o levantamento bibliográfico e a análise documental.

A primeira fase concentrou-se na identificação de obras, artigos científicos, dissertações, teses e outras produções especializadas relacionadas aos eixos centrais da pesquisa. As buscas foram realizadas no Google Acadêmico, no Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e na Biblioteca Digital Brasileira de Teses e Dissertações. A escolha dessas plataformas decorreu de sua ampla cobertura de produções científicas nacionais e internacionais, bem como da possibilidade de

acesso a diferentes gêneros acadêmicos.

Foram empregadas as palavras-chave “racismo”, “algoritmo”, “opacidade algorítmica”, “transparência”, “vieses”, “vigilância”, “policiamento preditivo”, “inteligência artificial”, “proteção de dados”, “reconhecimento facial”, “dados biométricos”, “biometria” e “seletividade penal”, dispostas isoladamente e em diferentes combinações. Os resultados encontrados foram filtrados conforme critérios de relevância temática, aderência ao problema de pesquisa, atualidade, adequação ao contexto brasileiro ou cearense e contribuição teórica para o estudo das tecnologias digitais no campo da segurança pública. Priorizaram-se produções publicadas nos últimos cinco anos, sem prejuízo da utilização de obras mais antigas quando indispensáveis à construção conceitual do trabalho.

O estágio seguinte consistiu na análise documental. Foram examinados relatórios, documentos institucionais, dados públicos, normas jurídicas, estudos especializados e materiais referentes à implementação de tecnologias de vigilância no Brasil e no Ceará. Entre os documentos centrais da investigação, destaca-se o relatório *Da construção de uma infraestrutura de vigilância à introdução do reconhecimento facial no Ceará*, elaborado na alçada do projeto *O Panóptico*, vinculado ao Centro de Estudos de Segurança e Cidadania (CESeC). A relevância desse levantamento decorre da sistematização de informações sobre investimentos em videomonitoramento, parcerias público-privadas, fluxos de dados, documentos administrativos, estruturas tecnológicas e riscos associados ao reconhecimento facial no estado.

O referencial teórico foi construído a partir de uma abordagem multidisciplinar que auxilia na compreensão do reconhecimento facial enquanto fenômeno sociotécnico e jurídico. Foucault (2001) fornece a base para o exame das sociedades disciplinares, ao permitir a análise das formas pelas quais o poder incide sobre os corpos e sobre a administração das populações. Deleuze (1992) amplia essa reflexão ao introduzir a noção de sociedade de controle, caracterizada pela vigilância contínua e pela fragmentação dos sujeitos em dados. Lyon (2018) contribui para o entendimento do processo de datificação da vida social, enquanto Rodotà (2008) elucida a relação entre a dignidade digital e os limites do poder informacional.

No âmbito dos estudos raciais e da crítica à tecnologia, Carneiro (2023) colabora com a formulação do dispositivo de racialidade, categoria fundamental para a compreensão do racismo como estrutura de poder. Benjamin (2019), por sua vez, oferece o conceito de *New Jim*

Code, que permite compreender como a segregação racial é atualizada e reproduzida por novas tecnologias e algoritmos supostamente neutros. No contexto brasileiro, Silva (2024) densifica esse debate ao discutir o racismo algorítmico, entendido como a reprodução de desigualdades raciais por meio de sistemas automatizados.

A pesquisa também mobiliza autores dedicados ao estudo dos algoritmos, da inteligência artificial e da opacidade algorítmica. Russell e Norvig (2010), Searle (2006), Frazão (2019; 2020; 2021; 2023), Pasquale (2016) e outros estudiosos foram utilizados para delimitar conceitos como algoritmo, aprendizado de máquina, inteligência artificial, *big data*, *big analytics*, caixa-preta e opacidade algorítmica. A análise dos vieses foi construída com apoio em Tversky e Kahneman (2012), bem como em autores que discutem heurísticas, distorções cognitivas e sua transposição para sistemas computacionais. A teoria do etiquetamento e a criminologia crítica foram incorporadas por meio de Becker (2008), Goffman (1981), Lemert (1967) e Misse (1999; 2006; 2008; 2009; 2010), cujas contribuições viabilizaram a compreensão da produção social da suspeição, da identidade desviante e da sujeição criminal.

A inteligência artificial generativa Gemini foi utilizada exclusivamente para fins de revisão ortográfica e gramatical. O uso da ferramenta restringiu-se ao suporte linguístico, sendo-lhe vedada a criação de conteúdo autônomo. Além disso, as sugestões foram submetidas à conferência humana e, em diversos casos, descartadas. Desse modo, preservou-se integralmente a autoria intelectual da pesquisa, assim como a responsabilidade pela seleção bibliográfica, análise documental, construção argumentativa e pelas conclusões apresentadas.

A estrutura da investigação acompanha o percurso metodológico e argumentativo delineado anteriormente. O primeiro capítulo dedica-se à construção do trajeto teórico concernente à sociedade de controle e à arquitetura tecnológica da vigilância contemporânea. Parte-se da sociedade disciplinar foucaultiana, caracterizada por instituições de confinamento, vigilância hierárquica e docilização de corpos, para, em seguida, alcançar a formulação deleuziana das sociedades de controle, fundadas na circulação contínua de dados e na vigilância difusa. Na sequência, examina-se a relação entre medo, securitização e expansão tecnológica para fins de segurança pública. Ao final, o capítulo investiga o uso da tecnologia como instrumento de controle social.

O segundo capítulo volta-se à análise dos sistemas inteligentes. Inicialmente, são

examinados os algoritmos, desde modelos simples até estruturas complexas baseadas em aprendizado de máquina. Em seguida, delimita-se o conceito de inteligência artificial e discutem-se as questões éticas que permeiam o vínculo entre humanos e máquinas. O capítulo também aborda o debate entre sintaxe e semântica, com destaque para os limites cognitivos das inteligências artificiais e para sua dependência em relação aos dados e parâmetros que as alimentam. Outrossim, são analisados vieses, heurísticas e formas de transposição de preconceitos humanos ao *design* tecnológico. A partir dessa base, desenvolve-se o diálogo sobre racismo algorítmico, opacidade e responsabilidade pelas decisões automatizadas.

O terceiro capítulo aplica a reflexão ao caso cearense. A princípio, descreve-se o funcionamento das tecnologias de reconhecimento facial e as condições que influenciam a confiabilidade desses sistemas. Posteriormente, analisa-se a trajetória da infraestrutura de vigilância no Ceará. A discussão avança para a sobrerrepresentação da população negra nas estatísticas criminais do estado, articulando-se com teorias como o etiquetamento e a sujeição criminal. Por fim, o capítulo examina os desafios impostos pela Lei Geral de Proteção de Dados, a lacuna regulatória relativa à segurança pública e a necessidade de salvaguardas voltadas à transparência, à auditabilidade, ao controle externo e à contestabilidade das decisões algorítmicas.

Ao final, constatou-se que o reconhecimento facial, quando incorporado às políticas de segurança pública, concentra riscos que ultrapassam a dimensão técnica. A investigação permitiu apreender que esses sistemas se inserem em uma racionalidade de controle sustentada pela estigmatização de pessoas e territórios, reforçando dinâmicas históricas de exclusão. Verificou-se, ainda, que a opacidade algorítmica dificulta a compreensão dos critérios que orientam alertas, correspondências biométricas e decisões derivadas de sistemas automatizados, reduzindo a capacidade de contestação dos sujeitos atingidos. No caso cearense, a combinação entre modernização tecnológica, desigualdade racial, seletividade penal e fragilidade normativa indica a possibilidade concreta de reprodução de práticas discriminatórias.

Concluiu-se, dessa forma, que a adoção de tecnologias de reconhecimento facial na segurança pública exige controle humano rigoroso, mecanismos institucionais de responsabilização, auditorias independentes, transparência e parâmetros normativos capazes de impedir que a eficiência tecnológica seja utilizada como justificativa para a criminalização de minorias sociais. O exame da realidade cearense demonstrou que a introdução de sistemas biométricos em políticas públicas de segurança demanda uma avaliação crítica de seus efeitos

sobre direitos fundamentais. Nesse sentido, o estudo reafirma que tecnologia e justiça não podem ser pensadas separadamente; ao revés, faz-se necessário garantir que as inovações tecnológicas sejam empregadas no desenvolvimento de sociedades mais equitativas.

2 A ARQUITETURA TECNOLÓGICA DA SOCIEDADE DE CONTROLE

Durante os séculos XVII e XVIII, as instituições de confinamento visavam à produção de corpos dóceis e úteis, com o propósito de satisfazer as demandas da economia e do Estado (Foucault, 2001). Para esse fim, valiam-se de mecanismos de vigilância, controle hierárquico e sancionatório, circunscritos a espaços rigorosamente demarcados (Foucault, 2001). No limiar do século XX, esses arranjos entraram em crise, permitindo o surgimento de novas formas de exercício do poder (Deleuze, 1992). No decorrer das últimas décadas, essas transformações nas dinâmicas de controle social culminaram na ruptura com os modelos institucionais que estruturavam a modernidade¹ (Deleuze, 1992), favorecendo a emergência de aparatos de vigilância mais difusos.

Em *Post-scriptum sobre as sociedades de controle*, Deleuze (1925-1995) teoriza que o declínio desses espaços de clausura não denota uma emancipação social plena, mas, antes, o prenúncio de um novo regime de poder. Ele postula que essas instituições “estão condenadas, num prazo mais ou menos longo. Trata-se apenas de gerir sua agonia e ocupar as pessoas, até a instalação das novas forças que se anunciam” (Deleuze, 1992, p. 220).

O presente capítulo se propõe a analisar essa alteração de paradigma. Partindo da herança teórica de Foucault (1926-1984) e de sua formulação de sociedade disciplinar, explorar-se-á a gênese das sociedades de controle, conforme proposta por Deleuze (1992). O argumento central sustenta que as sociedades de controle estão alicerçadas em práticas de conformação comportamental. Nessa nova ordem, os sujeitos são progressivamente convertidos em “divíduos” (Deleuze, 1992), isto é, entidades fragmentadas em dados e métricas, sujeitas a uma vigilância constante.

A análise desse processo é indispensável para compreender o reconhecimento facial como uma das expressões contemporâneas da racionalidade de controle. Antes de funcionar como ferramenta isolada de identificação biométrica, essa tecnologia integra um percurso

¹ No plano filosófico, a modernidade designa o processo de rompimento com a tradição teológica e metafísica que instaura a primazia do sujeito racional. Desde o pensamento cartesiano (Descartes, 2005), o homem é concebido como fundamento do conhecimento e medida de todas as coisas. Essa inflexão antropocêntrica inaugura o projeto iluminista de libertação pela razão (Kant, 2022), que associa o progresso humano à confiança no pensamento crítico, na ciência e na técnica. No sentido jurídico, a modernidade representa a consolidação do direito racional e estatal, estruturado em torno da legalidade, da igualdade formal e da previsibilidade normativa. Inspirado no contratualismo e no racionalismo (Hobbes, 2014; Locke, 2019; Rousseau, 2017), o direito moderno se legitima pela vontade humana, e não mais por fundamentos divinos. A codificação, a autonomia da esfera jurídica e a supremacia da lei simbolizam a passagem do arbítrio soberano ao império da norma (Kelsen, 2009). O Estado de Direito nasce, assim, como produto da crença na razão enquanto instrumento de organização social.

histórico em que o poder passa a depender de procedimentos automatizados de classificação. Por essa razão, a discussão sobre opacidade algorítmica e racismo exige, a princípio, a compreensão do ambiente político e tecnológico que torna possível a transformação de corpos em dados e de dados em critérios de suspeição.

Busca-se demonstrar, nesse sentido, como a emergência de um poder tecnológico, articulada à lógica do terror, serviu de catalisador para a expansão de aparatos de vigilância em massa, legitimando a invasão da esfera privada sob o pretexto da segurança coletiva. Essa racionalidade estabelece as bases para o desenvolvimento de tecnologias biométricas que ampliam a capacidade estatal de monitoramento e intensificam os riscos de discriminação, sobretudo quando aplicadas em sociedades atravessadas por desigualdades raciais.

Inicialmente, o foco de análise recairá sobre a transição do poder disciplinar para a conceituação deleuziana da sociedade de controle, além de suas características distintivas. Em seguida, o capítulo investigará como o medo e a vigilância em massa naturalizam esse novo regime de controle. Por fim, será construída uma ponte argumentativa que abordará as expressões materiais desse poder, com enfoque na tecnologia como infraestrutura de monitoramento e classificação social.

2.1 Da sociedade de disciplina...

O poder, enquanto fenômeno sociopolítico, busca sua legitimação por meio de estratégias diversas destinadas a assegurar a aceitação de sua autoridade (Burdeau, 1959, p. 186), entre as quais se pode mencionar o controle de corpos e informações (Martins *et al.*, 2024). Por essa razão, a compreensão contemporânea das tecnologias de vigilância, e, mais amplamente, dos regimes de poder que as sustentam, exige a contextualização histórica da passagem das sociedades disciplinares para as sociedades de controle. No plano conceitual, as formas de poder que organizam a vida social no Ocidente têm em Foucault (1926-1984) um de seus principais pontos de partida.

Em sua obra seminal *Vigiar e Punir* (Foucault, 2001), a conceituação da sociedade de soberania, predominante até o início da modernidade, expõe a primeira modalidade de exercício do poder. Nessas sociedades, historicamente associadas às formações monárquicas, o poder encontra-se centralizado na figura do soberano, cuja autoridade se expressa no direito de decidir sobre a vida e a morte de seus súditos. Trata-se de um poder que se manifesta, positivamente, “sobre a vida, que empreende sua gestão, sua majoração, sua multiplicação, o

exercício, sobre ela, de controles precisos e regulações de conjunto” (Foucault, 2005, p. 129).

Seu exercício ocorre de maneira externa e visível, e sua natureza revela-se essencialmente punitiva (Foucault, 2001). A relação estabelecida não é a da disciplinarização minuciosa dos corpos, como se verificará nas sociedades posteriores, mas sim a do vínculo de obediência a um determinado líder. Os dispositivos primordiais dessa forma de poder são a coerção e o medo, representantes da força indivisa exercida sobre o súdito.

Na sociedade de soberania, o controle social se realiza pela ostentação do sofrimento e pela teatralidade da violência legítima. Sua ação é reativa, pois intervém sobre fatos pretéritos, isto é, após a ocorrência do crime, quando a ordem foi rompida. Por esse motivo, os corpos servem de suporte para a punição exemplar, inclusive mediante a pena capital. O suplício e a execução penal correspondem às modalidades mais espetaculares e diretas de controle, por meio das quais se reafirma a transcendência do poder do soberano (Foucault, 2001).

A inflexão das sociedades de soberania para as sociedades disciplinares deu-se entre os séculos XVII e XVIII (Foucault, 2001, p. 173). Diferentemente do poder soberano, a disciplina se materializa nos corpos dos sujeitos individualizados (Pogrebinski, 2004, p. 190). Ela age internamente, a partir de instituições hierarquizadas e espacialmente delimitadas (Foucault, 2001).

Nesse arranjo, o poder é exercido pela imposição de normas sociais predefinidas, que demarcam o espaço e o tempo dos indivíduos. Para Foucault (2001, p. 143), “o poder disciplinar é com efeito um poder que, em vez de se apropriar e retirar, tem como função maior ‘adestrar’”. Seu objetivo não é punir o corpo, mas, antes, moldá-lo e torná-lo útil e dócil, ajustado a funções específicas e a padrões de normalidade.

O mecanismo emblemático da sociedade disciplinar é a vigilância hierárquica e contínua (Foucault, 2001, p. 143), visualizada no panóptico,² cuja arquitetura garante a indivisibilidade e a automaticidade da vigília. Esse aparelho equivale a um “olho perfeito a que

² Estrutura arquitetônica “[...] de implantação dos corpos no espaço, de distribuição dos indivíduos em relação mútua, de organização hierárquica, de disposição dos centros e dos canais de poder, de definição de seus instrumentos e de modos de intervenção [...]” (Foucault, 2001, p. 177). Essa figura circular permite a um único vigilante posicionar-se em uma torre central, longe da vista dos demais ocupantes, e observar todos os presentes. Dispostos em celas igualmente circulares, os detentos não sabem se estão ou não sendo vigiados. A incerteza e a sensação de vigilância constante são eficientes na medida em que influenciam o comportamento dos monitorados, instigando sua submissão e autodisciplina.

nada escapa e centro em direção ao qual todos os olhares convergem” (Foucault, 2001, p. 146), que permite “um controle interior, articulado e detalhado” (Foucault, 2001, p. 145). Seu objetivo é, precisamente, “induzir no detento um estado consciente e permanente de visibilidade” (Foucault, 2001, p. 191), o que assegura o funcionamento automático do poder (Foucault, 2001, p. 191).

Escolas, quartéis, fábricas, hospitais e prisões constituem o laboratório desse modelo de sociedade, amparado em estratégias de adestramento e na lógica de clausura (Foucault, 2001). Cada instituição corresponde a um espaço de socialização, no qual o indivíduo disciplinado é confinado e submetido a um regime de obediência: o espaço escolar forma o estudante, o hospital disciplina o doente, o quartel treina o soldado, a fábrica molda o operário e a prisão corrige o delinquente (Foucault, 2001).

Essa gramática disciplinar não se impõe pela violência direta, mas por uma incitação discreta (Sabot, 2017, p. 21) que conforma corpos e condutas. Com o auxílio de dispositivos disciplinares como o panóptico, o poder torna-se visível para o vigilante e inverificável para o vigiado, induzindo um estado de consciência permanente (Foucault, 2001). Fora desses espaços, entretanto, a lógica disciplinar é enfraquecida, ainda que a multiplicidade de instituições garanta certa continuidade aos moldes de confinamento que compõem a rede de domínio social.

Esse modo de organização humana, embora eficaz no contexto do capitalismo industrial, apresentava limitações diante das transformações políticas, econômicas e tecnológicas do século XX (Capovilla, 2019). Isso porque a disciplina não era onipresente; seu funcionamento pressupunha fronteiras relativamente claras entre dentro e fora³ (Hardt, 2000). Assim, após a Segunda Guerra Mundial, os dispositivos disciplinares descritos por Foucault entraram em crise (Deleuze, 1992, p. 219-220), uma vez que “as disciplinas de confinamento deixaram de ser o centro irradiador do *modus vivendi* para o conjunto da sociedade” (Capovilla, 2019, p. 265). Esse colapso preparou a passagem para formas mais difusas de controle, nas

³ Segundo Hardt (2000), a distinção moderna entre as esferas interna e externa ao indivíduo vincula-se a uma série de processos de subjetivação. Na configuração das sociedades disciplinares, a identidade do indivíduo era forjada no interior de instituições de enclausuramento – como o hospital, a família e a prisão –, o que conferia às subjetividades uma estrutura estável, pois cada ambiente possuía regras e objetivos específicos. Quando estava “dentro” da fábrica, o indivíduo era um operário; na escola, um aluno. Em contrapartida, quando estava “fora” desses limites, o indivíduo possuía certa liberdade, uma vez que o poder não chegava a esses locais. Com a ascensão da sociedade de controle, porém, a produção dos sujeitos ultrapassa os limites institucionais. Nesse cenário, já não existe um espaço social que não esteja sendo monitorado, precificado ou influenciado por mecanismos de controle, o que torna as subjetividades voláteis.

quais a observação deixa de depender exclusivamente da clausura.

2.2 ...à sociedade de controle

É nesse ponto que Deleuze (1992) anuncia a emergência de um novo diagrama de poder. Segundo ele, o modelo de confinamento tornou-se insuficiente frente às novas maneiras de circulação do capital, às transformações do trabalho e à emergência de tecnologias informáticas (Deleuze, 1992, p. 223). A disciplina, em que pese ainda presente, já não era capaz de abranger a complexidade das sociedades em rede⁴ (Castells, 1999; 2003), marcadas pela mobilidade e pela comunicação instantânea (Garcia, 2019). Diante disso, o panóptico mostrou-se inadequado para descrever os novos circuitos de vigilância que se insinuavam.

Como consequência, o centro de gravidade da teoria foucaultiana foi alterado: “são as sociedades de controle que estão substituindo as sociedades disciplinares” (Deleuze, 1992, p. 220). Se a disciplina funciona por moldes, em um processo fixo que enclausura os indivíduos em espaços rígidos e homogêneos, o controle desenvolve-se de forma dispersa, por modulações, “como uma moldagem auto-deformante que mudasse continuamente” (Deleuze, 1992, p. 221).

O eixo da coerção é deslocado para uma vigilância difusa e ilimitada (Deleuze, 1992, p. 224), na qual o confinamento é superado pela circulação incessante de dados. A passagem da disciplina ao controle marca, portanto, uma mutação na forma de exercício do poder: do espaço fechado para o espaço aberto, de instituições rígidas à fluidez e ubiquidade.

Essa mudança, porém, não implica a extinção das disciplinas, mas a sua reconfiguração. Hardt (2000) enfatiza que o que se perde é a centralidade exclusiva dos confinamentos, e não a sua existência. Para o autor, “os muros das instituições estão desmoronando de tal maneira que suas lógicas disciplinares não se tornam ineficazes mas se encontram, antes, generalizadas como formas fluidas através de todo o campo social” (Hardt, 2000, p. 357).

Nesse contexto, a disciplina é diluída e reinventada em dispositivos indistintos, dissolvendo a divisa entre dentro e fora (Hardt, 2000, p. 360). O poder disciplinar, antes

⁴ De acordo com Castells (2003, p. 286-287), a sociedade em rede corresponde à estrutura social organizada em torno de redes de informação e comunicação digital. O modelo, impulsionado pela globalização, é mediado pela tecnologia microeletrônica, notadamente a internet. Para o sociólogo, a “Internet é o coração de um novo paradigma sociotécnico, que constitui na realidade a base material das nossas vidas e de nossas formas de relação, de trabalho e de comunicação. O que a Internet faz é processar a virtualidade e transformá-la em nossa realidade [...]” (Castells, 2003, p. 286-287).

dependente de instituições para ser exercido de modo estável, adquire a natureza de controle, tornando-se imanente às práticas sociais. Contrariamente ao panoptismo foucaultiano, o controle não reconhece exterioridade, pois nele todos são, simultaneamente, vigilantes e vigiados.

Com isso, o poder se expande e atravessa todos os domínios da vida social, superando fronteiras físicas e institucionais. A docilidade e a vigilância permanecem, mas agora se inserem em espaços abstratos, o que permite a formulação de uma “sociedade mundial de controle” (Hardt, 2000, p. 372). Do ponto de vista técnico-político, a chave dessa passagem é a informática como infraestrutura de poder.

Ao contrário da disciplina, que confinava corpos em moldes, o controle fragmenta indivíduos em unidades de informação (Deleuze, 1992). Como observa Garcia (2019, p. 533), “as sociedades de controle são reguladas por uma linguagem numérica”, na qual a vigilância se efetiva por meio da extração e do cruzamento de dados. Deleuze (1992, p. 222) assevera que “o essencial não é mais uma assinatura nem um número, mas uma cifra: a cifra é uma senha”. Surge, a partir dessa observação, o conceito de “divíduo” (Deleuze, 1992), manifestação da lógica de controle que condiciona a subjetividade contemporânea.

Na sociedade disciplinar, o “indivíduo” era concebido como uma totalidade coesa e indivisível, formada de fora para dentro por intermédio da socialização e do confinamento (Deleuze, 1992, p. 222). Em contrapartida, o “divíduo” consiste em um conjunto de amostras, dados, mercados ou bancos (Deleuze, 1992, p. 222) divisíveis, quantificáveis e manipuláveis por sistemas informáticos. No controle, a vida é convertida em fragmentos informacionais, classificáveis por algoritmos⁵ e passíveis de tratamento automatizado. Esse é o núcleo que, mais adiante, permitirá discutir a datificação e a opacidade algorítmica, mas que, desde sua gênese, delimita o salto histórico do corpo moldado ao corpo amostrado.

Esse fenômeno assinala um movimento no exercício do poder que excede os limites da biopolítica (Foucault, 2001), consistente no conjunto de técnicas e saberes, incluindo aspectos da vida biológica, destinados à administração e ao controle dos cidadãos do século XVIII. Por conseguinte, a dinâmica atual adentra no que Han (2018) qualifica como psicopolítica.

⁵ De acordo com Frazão (2020, p. 32), algoritmos “são os instrumentos por meio dos quais os dados são processados e podem ser revertidos em resultados (*outputs*) a serem utilizados para as mais diversas finalidades”.

A biopolítica mantém uma correlação intrínseca com o regime disciplinar, cuja organização se manifesta sobre “corpos” (Han, 2018, p. 31). De maneira diversa, a psicopolítica é a forma contemporânea de exercício do poder, característica de regimes neoliberais. Essa modalidade de dominação se comporta como “alma” (Han, 2018, p. 31), atuando diretamente sobre a *psique* dos indivíduos.

Sob a influência da psicopolítica, o sujeito contemporâneo busca na tecnologia a reconstrução de sua própria identidade. Desse modo, o processo de fragmentação do “indivíduo” em “divíduo” resulta na criação de uma nova forma de coletividade, que se encontra apoiada na mensuração estatística (Portella, 2021). O que se controla não é mais o sujeito enquanto presença física em um espaço fechado, mas sua constituição como um emaranhado de dados.

As práticas atualmente observadas em algoritmos de reconhecimento facial, por exemplo, já eram esboçadas na noção de “divíduo”. O conceito, como visto, expressa a fragmentação dos sujeitos em dados e perfis estatísticos, articulando-se ao manejo de comportamentos em um sistema global de monitoramento e sujeição (Deleuze, 1992). Trata-se de uma mutação que não elimina a disciplina (Hardt, 2000; Deleuze, 1992), mas a conecta a um raciocínio mais abrangente, no qual os fluxos de informações são seus eixos centrais.

Todavia, a sociedade de controle não altera somente condutas, mas também a relação entre poder e temporalidade. As disciplinas operam em tempos lineares e previsíveis, corrigindo o erro após o desvio. A lógica de controle, por sua vez, funda-se na intervenção prospectiva, isto é, na antecipação de riscos e probabilidades (Sabot, 2017). Nesse novo arranjo, a segurança, e não mais a lei, torna-se o princípio ordenador das relações sociais.

Menezes Neto e Moraes (2018) destacam que essa situação permite simular futuros e manipular atitudes presentes. Isso porque o controle não apenas vigia o que acontece, mas antecipa o que pode vir a acontecer, dando origem a uma racionalidade preditiva (Sabot, 2017). Os autores advertem, ainda, que antever um futuro inexistente pode culminar na normalização de um “pré-crime” e na erosão da democracia (Menezes Neto; Moraes, 2018, p. 1152).

De maneira análoga, Wang (2022) sustenta que o discurso estatístico, intrínseco ao policiamento preventivo, apresenta o fenômeno criminal como um evento de natureza biológica ou inexorável, dissociado da autonomia individual ou das condicionantes sociais. A lógica da antecipação, segundo a autora, promove a patologização da população negra ao transmutar

dados de controle social em indicadores de periculosidade. Por conseguinte, a estruturação de métricas para uma persecução penal antecipada perpetua a racialização histórica da criminalidade, consolidando diagnósticos marcados por vieses discriminatórios e imprecisões analíticas.

Apesar dos alertas, a fabricação do risco permanece como componente estruturante da era da vigilância tecnológica. Os ataques aos Estados Unidos em 11 de setembro de 2001 simbolizam, no plano geopolítico, essa virada paradigmática (Bauman; Lyon, 2014; Duarte; Carvalho Netto, 2012). O evento é frequentemente mobilizado como marco da expansão da securitização global⁶ (Feldman, 2011), entendida como a construção de ameaças permanentes que legitimam medidas de emergência fora dos procedimentos políticos normais (Silva; Pereira, 2019).

A partir desse acontecimento, inaugurou-se uma “guerra contra o terror” (Feldman, 2007), na qual o inimigo, antes externo e de fácil identificação, é considerado invisível e onipresente. Nesse horizonte, o medo (Crawford, 2014), a suspeição (Menezes Neto; Morais, 2018) e a mundialização do controle (Hardt, 2000) tornam-se objetos de políticas concretas, como listas de observação, vigilância de fronteiras, coleta massiva de dados e uso de biometria (Martins *et al.*, 2024).

Bauman (2008) assinala que a política da intranquilidade, compreendida como a exploração, pelo poder político, dos medos dos cidadãos visando à manutenção da legitimidade estatal, reforça a aceitação social desses mecanismos intrusivos de controle. Essa vulnerabilidade psicológica coletiva impele a busca por vias alternativas de proteção, que comumente se revelam ilusórias ou ineficazes dada a natureza volátil da ameaça (Bauman, 2008). Como será visto adiante, em contextos marcados por violência urbana e insegurança social, o risco, mesmo hipotético, justifica medidas de monitoramento permanente, e tecnologias preditivas são apresentadas como soluções inevitáveis, conquanto impliquem profundas restrições à liberdade (Martins *et al.*, 2024).

Nessa linha de raciocínio, ao distinguir o “direito penal do cidadão”, orientado à reafirmação da norma violada, do “direito penal do inimigo”, destinado à contenção preventiva

⁶ A securitização expande o conceito de setor de segurança para domínios emergentes, a exemplo do espaço cibernético. Esse mecanismo classifica a esfera digital como um setor autônomo de risco. Do mesmo modo, permite que a ameaça midiática seja rapidamente convertida em política de segurança repressiva sem o escrutínio dos procedimentos normativos. Em virtude disso, o discurso da segurança torna-se um capital político que justifica o aumento do poder coercitivo estatal e o recrudescimento penal (Silva; Pereira, 2019).

de sujeitos considerados perigosos, Jakobs (2009) desvenda um modelo jurídico que antecipa a punição em nome da segurança. Na esfera jurídica, a culpa como parâmetro analítico cede lugar aos cálculos probabilísticos que agora gerenciam o transgressor do contrato social (Bauman, 2008). Reduzido a um risco potencial, o inimigo é considerado indigno do estatuto de pessoa (Bauman, 2008) e, por conseguinte, destituído de seus direitos como cidadão (Pinto, 2015). Consagra-se, então, a passagem de um Estado de Direito a um Estado de Vigilância (Silva, 2024), em que a suspeição substitui a sanção.

Beck (1992) sustenta que esse cenário origina uma sociedade de risco, caracterizada pela produção sistemática de ameaças globais decorrentes do progresso tecnológico e da modernização. Nesse molde social, os riscos deixam de ser pessoais e adquirem uma escala coletiva e global (Beck, 1992). Motivada pelo clamor social, essa conjuntura repercute no campo normativo-político, no qual o Direito Penal é mobilizado como ferramenta de gestão de riscos, especialmente por meio da tipificação de crimes de perigo abstrato (Beck, 1992).

O resultado é um Direito Penal que abdica de sua função de *ultima ratio* e se converte em um braço normativo da segurança pública, assumindo a posição de simples técnica de controle policial preditivo (Morozov; Bria, 2019). Bechara (2008) demonstra que a pena, nesse quadro, deixa de ter natureza retributiva ou educativa e assume um caráter meramente simbólico. Ela tranquiliza a opinião pública e projeta segurança sobre o futuro, mesmo à custa do alargamento de tipos penais e da flexibilização de garantias e de princípios fundamentais, que “passam a ser vistos como sutilezas e barreiras para a eficiência do poder punitivo do Estado” (Bechara, 2008, p. 423).

Essa racionalidade fornece o pano de fundo necessário para compreender a consolidação de tecnologias invasivas como dispositivos paradigmáticos em uma sociedade marcada pela desconfiança. Sistemas como o reconhecimento facial são aparatos que possibilitam a concretização desse controle, cuja materialização será analisada na seção seguinte.

2.3 O uso da tecnologia como instrumento de controle social

A racionalização e a classificação de indivíduos, derivadas de uma cultura de vigilância⁷ (Lyon, 2018, p. 153-154), constituem um atributo característico da modernidade

⁷ A cultura de vigilância designa uma variedade de formas de monitoramento e coleta de dados que ultrapassam a fiscalização tradicional, expressa na força externa e coercitiva, e se tornam parte do cotidiano social (Lyon, 2018).

(Duarte; Nunes; Lima, 2023, p. 13; Lyon, 2018). No entanto, o desenvolvimento de metodologias e instrumentos de ordenação social não se restringe a esse período histórico (Duarte; Nunes; Lima, 2023, p. 13; Brayne, 2022).

A propensão para o manejo populacional, que resulta na criação de diferentes ferramentas de controle, é um componente intrínseco à estruturação das sociedades humanas (Duarte; Nunes; Lima, 2023). Exemplos disso residem em civilizações antigas, notadamente em Roma e no Egito, onde a manutenção sistemática de catálogos e registros escritos era essencial para o gerenciamento eficaz das massas demográficas (Duarte; Nunes; Lima, 2023, p. 13).

Na perspectiva de Deleuze (1992), cada etapa da organização humana é acompanhada por maquinários de controle moldados pelas racionalidades políticas que lhes são contemporâneas. Nesse percurso, a coleta de dados e o monopólio da informação revelam-se indispensáveis à preservação da autoridade governamental e à manutenção da hierarquia social (Foucault, 1991; Brayne, 2022; Duarte; Nunes; Lima, 2023; Harari, 2024). A passagem dos registros manuais (Lyon, 1994; Weller, 2012) para as estruturas físicas de observação e, posteriormente, para os dispositivos eletrônicos de monitoramento, a exemplo de câmeras de vigilância (Ferreira, 2024, p. 70), traduz um processo de incorporação da tecnologia à gestão da vida coletiva (Duarte; Nunes; Lima, 2023; Frois, 2015).

Com o advento das sociedades industriais (Duarte; Nunes; Lima, 2023, p. 14), inaugurou-se uma nova era na relação entre Estado, tecnologia e controle social. Cole (2001) ressalta que a rápida expansão dos centros urbanos, o crescimento demográfico e o desenvolvimento tecnológico impuseram novas exigências ao exercício do poder. Isso porque a capacidade humana mostrou-se insuficiente para observar a totalidade de corpos dispersos em determinado espaço.

Diante dessa limitação, os aparatos tecnológicos destinados à vigilância foram formalmente incorporados à administração pública moderna (Duarte; Nunes; Lima, 2023). Nesse contexto, foram concebidos dispositivos de monitoramento e regulação populacional mais sofisticados, associados ao reforço da capacidade repressiva e operacional do aparato policial (Cole, 2001).

Valendo-se desses instrumentos, os Estados desenvolveram novas estratégias, semelhantes aos atuais sistemas de fiscalização (Giddens, 1990), para a coleta ordenada e

massiva de informações sobre indivíduos e grupos sociais. Harari (2024) assevera que essas redes tecnológicas automatizaram a função ordenadora antes desempenhada pela burocracia humana. O autor adverte que essa sofisticação da linguagem técnica pode conduzir a um controle imperceptível, uma vez que a complexidade dos sistemas de tecnologia tende a afastar o elemento humano dos centros decisórios.

Em um panorama marcado pela complexidade da gestão social em larga escala, Foucault (2008) introduziu o conceito de governamentalidade. O termo descreve a emergência de um conjunto de instituições, procedimentos, análises, reflexões, cálculos e táticas, cujo escopo primário é centrado na regulação eficiente das populações, tendo como seu “instrumento técnico essencial os dispositivos de segurança” (Foucault, 2008, p. 143-144). Conforme será visto adiante, a compreensão regulatória que emerge desse arcabouço, quando associada às tecnologias digitais, se apoia na gestão probabilística e na ingerência sobre comportamentos (Rouvroy; Berns, 2013).

Essa perspectiva permanece sendo um dos principais fundamentos da técnica moderna (Lyon, 2003). Além disso, ela explica por que o avanço das tecnologias securitárias tende a ampliar, e não a reduzir, a intervenção estatal (Frazão, 2020, p. 28). À medida que os dispositivos de segurança se integram às práticas de classificação social⁸ (Lyon, 2003), a vigilância assume uma função determinante na forma pela qual operam as instituições contemporâneas (Monahan; Murakami-Wood, 2018, p. xix).

Com efeito, a constituição de acervos cadastrais e bases de dados populacionais representa o marco inicial da integração entre Estado, tecnologia e vigilância (Lyon, 2003; Giddens, 1981). Censos, registros civis e fichamentos policiais compuseram um arcabouço documental que permitiu ao Estado moderno reconhecer e ordenar a população segundo critérios de utilidade, produtividade e periculosidade (Duarte; Nunes; Lima, 2023).

Giddens (1981) identifica essa conjuntura como um estágio de vigilância administrativa. Nesse modelo, “a vigilância como mobilização do poder administrativo – através do armazenamento e controle de informação – é a forma primária de concentração de recursos autoritários envolvidos na constituição do Estado-nação” (Giddens, 1981, p. 181). Foi dentro desse arcabouço que o Estado teve sua capacidade de vigiar, controlar, organizar,

⁸ O processo de classificação social, ou *social sorting*, corresponde à própria noção de vigilância moderna, que separa os indivíduos em diferentes categorias segundo graus de valor e de risco à lei e à ordem (Lyon, 2003).

fiscalizar e punir potencializada por dispositivos tecnológicos (Benjamin, 2019).

O cenário da vigilância administrativa, que exigia “a observação imediata, o trabalho centralizado de coleta de informações e a produção de arquivos detalhados sobre os indivíduos” (Duarte; Nunes; Lima, 2023, p. 20) perdurou até meados dos anos 1970 (Rule, 1974). Durante esse período, o panóptico, concebido por Bentham e analisado por Foucault (2001), serviu como a metáfora arquitetônica e conceitual que melhor explicava as formas de regulação social assentadas em uma observação centralizada e hierarquizada. Contudo, a iminente revolução algorítmica desmantelou, em parte, esse modelo de administração da vida social, conforme apontado por Deleuze (1992).

De acordo com Lyon, Haggerty e Ball (2012, p. 1), os últimos 40 anos foram marcados pelo “desenvolvimento de infraestruturas materiais, empresariais e governamentais suportadas por sistemas tecnológicos de análise e cruzamento de dados” que alteraram profundamente as possibilidades de observação e controle da sociedade. O surgimento da computação, sobretudo com a microinformática e a internet (Lemos, 2021, p. 194), intensificou o uso de aparatos de vigilância.

Nessa etapa, os instrumentos de segurança passam a ser mediados por algoritmos (Lyon, 2003; Morozov, 2015; Zuboff, 2018), o que inclui, por exemplo, “vastos circuitos de câmeras e sistemas de aprendizado de máquina (machine learning)” (Duarte; Nunes; Lima, 2023, p. 20). Essa nova vigilância é exercida de maneira remota, involuntária, automatizada e preventiva (Marx, 2002, p. 20).

Assim, entre o final do século XX e início do século XXI, iniciou-se um processo de digitalização (Brayne, 2022) e, de maneira mais significativa, de datificação (Mayer-Schöenberger; Cukier, 2013) da vida humana. Essa situação foi intermediada por computadores e máquinas informáticas típicas das sociedades de controle (Deleuze, 1992, p. 223). Em coerência com o raciocínio deleuziano, a datificação diz respeito à transformação de comportamentos, interações e demais aspectos da experiência humana em dados quantificáveis, passíveis de rastreamento e de análise preditiva (Mayer-Schöenberger; Cukier, 2013, p. 28).

Nessa conformação, como antecipava Deleuze (1992), a vigilância é distribuída e difusa (Lyon, 2014; Barassi, 2020), sendo aplicada, inclusive, no âmbito policial (Garfinkel, 2001). Consoante discutido na seção anterior, a tecnologia, assim como a vigilância, é essencial para o exercício do poder, haja vista que possibilita a coleta e a manipulação de dados, o que,

por sua vez, influencia a ação humana (Deleuze, 1992).

Sob essa perspectiva, Burdon e Cohen (2021, p. 155) afirmam que a “difusão das redes digitais contribuiu para a ruptura de domínios disciplinares distintos”, proporcionando uma infraestrutura de vigilância capaz de observar, contínua e discretamente, “indivíduos móveis em ambientes dispersos” (Burdon; Cohen, 2021, p. 155).

Essa nova fase da vigilância tecnológica está associada a uma reestruturação da racionalidade econômica que Morozov (2015) denomina capitalismo de dados.⁹ A nomenclatura define um modelo de acumulação de capital fundado na extração e na mercantilização da informação digital. Essa infraestrutura econômica é suportada por repositórios de metadados, nos quais a coleta, o tratamento e o uso de dados pessoais se tornam o principal ativo de valor (Fraser; Jaeggi, 2020).

No mesmo sentido, Zuboff (2018) formaliza a associação entre acumulação econômica de dados e controle social com o conceito de capitalismo de vigilância. Para a filósofa, o *big data*¹⁰ funciona como uma condição e uma expressão dos regimes de opressão. Frazão (2019) coaduna-se com a autora estadunidense ao afirmar que o *big data* e o *big analytics*¹¹ são alguns dos meios que consolidam a vigilância informatizada como um pilar do século XXI.

O cerne do capitalismo de vigilância reside, então, na utilização da totalidade da experiência humana como matéria-prima (Zuboff, 2018), agora traduzida em dados comportamentais passíveis de mercantilização. Nessa acepção, os algoritmos assumem uma posição central nas mais diversas áreas da vida social (Bezerra; Coelho, 2022, p. 4). Diante desse cenário, Frazão (2020, p. 28) conclui que a economia movida a dados e o capitalismo de vigilância constituem “duas faces da mesma moeda pois, quanto maior a importância dos dados,

⁹ Nesse mesmo horizonte, Simon (1971) identifica a emergência de uma economia da atenção. A expressão descreve a atenção humana como um recurso escasso e valioso, sobretudo em um contexto de abundância de informações digitais. Em sociedades hiperconectadas (Magrani, 2018), plataformas de mídia e tecnologia competem para capturar e reter o foco, o tempo e o engajamento do usuário. Essa atenção é convertida em valor econômico a partir de recompensas psicológicas capazes de moldar comportamentos. Assim como no capitalismo de dados (Morozov, 2015), o objetivo da economia da atenção é lucrar com aspectos da experiência humana. Dessa maneira, ela cria as condições subjetivas que garantem a permanência dos indivíduos dentro do ecossistema de coleta característico do capitalismo de dados.

¹⁰ O termo diz respeito à gestão e análise de uma volumosa quantidade de dados, que podem ser estruturados, semiestruturados ou não estruturados (Magrani, 2018, p. 22). A relevância desses dados reside na possibilidade de extração de informações, função que é potencializada pelo aumento da capacidade de estocagem, busca, agregação e cruzamento de algoritmos e mecanismos computacionais (Boyd; Crawford, 2012).

¹¹ Para Frazão (2019, p. 337), o *big analytics* refere-se à “possibilidade de extrair, a partir dos dados, correlações, padrões e associações que possam ser consideradas informações”.

mais incentivos haverá para o aumento da vigilância e, por conseguinte, maior será a coleta de dados”.

A onipresença da coleta sistemática de dados, levada a cabo tanto pelo Estado quanto pelas grandes corporações privadas (Melo; Serra, 2022, p. 207), resulta em um “novo panóptico” ou “olho eletrônico” (Lyon, 1994). Esse processo está na base do conceito de sociedade de vigilância (Lyon, 1994), que abrange as múltiplas e crescentes esferas nas quais dados pessoais são coletados por agências administrativas, comerciais e de segurança (Lyon, 1994, p. ix).

A análise de Lyon (1994) indica que novas tecnologias conferem à vigilância um caráter mais fluido, complexo, constante e, sobretudo, imperceptível, em consonância com o que previa Deleuze (1992). Nesse sentido, a disseminação de instrumentos de monitoramento, a exemplo de tornozeleiras eletrônicas (Peron; Alvarez; Campello, 2018), organiza modos de controle social percebidos como mais toleráveis.

Esse processo resulta na maior aceitação social de aparatos invasivos, aumentando a capacidade de produção de corpos dóceis e desejáveis (Foucault, 2001; Peron; Alvarez; Campello, 2018). Consequentemente, o capitalismo de dados implementa formas ainda mais ubíquas de vigilância, extração, monetização e tomada de decisão automatizada, consolidando o poder nas mãos de Estados e das grandes empresas de tecnologia (Bezerra; Costa, 2022).

Dessa maneira, práticas de coleta massiva de dados, aliadas às novas tecnologias de monitoramento e processamento algorítmico, conduziram a uma nova modalidade de governança. Rouvroy e Berns (2010, 2013) descrevem essas técnicas como um novo saber estatístico, apoiado em dispositivos de detecção, classificação e avaliação antecipatória de comportamentos humanos. Esse fenômeno consagra aquilo que os autores denominaram governamentalidade algorítmica (Rouvroy; Berns, 2010). A referência a Foucault é justificada pela compreensão de que essa governamentalidade se realiza continuamente por meio de dispositivos de segurança, os quais sustentam o exercício do poder (Rouvroy; Berns, 2013).

A governamentalidade algorítmica pode ser entendida como um certo tipo de racionalidade (a)normativa ou (a)política, que repousa sobre a recolha, agregação e análise automática de dados em quantidade excessiva, de maneira a prever e regular ações futuras (Rouvroy; Berns, 2013). Seu poder reside fundamentalmente nos algoritmos de correlação estatística, articulados para um controle ou, mais precisamente, para uma antecipação de

condutas (Rouvroy; Berns, 2010). Caracteriza-se, assim, pela capacidade de interpretar os dados registrados a partir de critérios de normalidade ou anormalidade, interesse ou indiferença, visando prever, orientar e prevenir certos tipos de comportamentos.

No domínio da segurança pública, a governamentalidade algorítmica autoriza e, em muitos casos, exige a implementação de uma série de dispositivos de vigilância de caráter preditivo e/ou preventivo (Bruno, 2013). A expansão global da videovigilância, por exemplo, tem sido apoiada por um número crescente de governos e populações como forma de combate ao crime e à violência urbana (Bruno, 2013). Essa reorganização das políticas de planejamento e administração das cidades deu origem às cidades inteligentes (Magro; Fortes, 2021; Silva, 2024).

Nos espaços urbanos contemporâneos, a infraestrutura física é mediada por sistemas digitais de análise e processamento de dados aptos a monitorar fluxos populacionais e comportamentais em tempo real (Magro; Fortes, 2021, p. 304-305). Para essa finalidade, emprega-se uma multiplicidade de dispositivos autônomos de correlação estatística, incluindo câmeras de reconhecimento facial, sensores de inteligência artificial e algoritmos de aprendizado de máquina (Magro; Fortes, 2021, p. 308; Silva, 2024).

Magro e Fortes (2021, p. 305) postulam já ser possível vislumbrar a criação de projetos de cidades onipresentes, equipadas com redes que capacitam autoridades a monitorar integralmente tudo o que ocorre em seu território. A disseminação dessas tecnologias, que dissolvem as fronteiras entre observador e observado (Silva, 2024), inaugurou um momento de “policimento à distância” (Haggerty; Wilson; Smith, 2011). Como consequência, multiplicou-se a atuação de agentes públicos e privados nas tarefas de regulação social (Haggerty; Wilson; Smith, 2011). Sob essa ótica, a instalação de tecnologias como o videomonitoramento indica a constituição de um “panóptico eletrônico” que intensifica os dispositivos disciplinares de controle (Norris, 2003).

O policiamento preditivo¹² (Morozov; Bria, 2019; Pullen; Schefer, 2021; Brayne,

¹² Conforme expõe Brayne (2021, p. 74), o policiamento preditivo estrutura-se em quatro fases distintas: coleta, análise, intervenção e resposta. A etapa inicial corresponde à sistematização e organização dos dados disponíveis. Em seguida, procede-se à análise dessas informações, que pode variar desde modelos estatísticos elementares até procedimentos algorítmicos mais sofisticados. A terceira fase refere-se à intervenção policial, momento em que as previsões criminais orientam a definição estratégica do posicionamento das forças de segurança em determinado território. A etapa final consiste na reação dos indivíduos submetidos ao policiamento, que pode manifestar-se tanto pela desistência da prática delitiva quanto pelo deslocamento da atividade criminosa para outros espaços. Ao término desse ciclo, a autora ressalta que novos dados são produzidos, os quais servem de base para a elaboração

2021) consiste na aplicação direta dessa racionalidade. Ele pode ser definido como a utilização de procedimentos analítico-técnicos que, baseando-se em previsões estatísticas, identificam incidentes que exigem intervenção policial, permitindo a tomada de medidas preventivas (Pullen; Schefer, 2021, p. 105; Brayne, 2021). Os resultados desses procedimentos, possibilitados pela análise de dados e por algoritmos de aprendizado de máquina, incluem desde previsões relacionadas a locais prováveis para o cometimento de crimes até a probabilidade de um indivíduo praticar determinado delito (Pullen; Schefer, 2021). Seu objetivo é evitar ou reduzir a criminalidade, permitindo às autoridades identificar potenciais infratores antes mesmo que estes se manifestem como tais (Pullen; Schefer, 2021, p. 105).

Entretanto, apesar de sua expansão global, o aumento da videovigilância não possui correlação com a efetiva redução da criminalidade (Gill; Spriggs, 2005; Welsh; Farrington, 2008). Não obstante isso, a ineficácia desse instrumento não é suficiente para descartar o uso de medidas securitárias (Bruno, 2013). Essa situação indica que o valor primário da tecnologia de controle, no atual estágio da sociedade, reside menos em sua eficiência empírica e mais na sua função ideológica, que legitima a expansão do poder estatal e corporativo (Bruno, 2013).

A trajetória de evolução tecnológica indica que, desde o modelo disciplinar clássico (Foucault, 2001), até os elementos de vigilância inerentes às sociedades de controle (Deleuze, 1992), o uso da tecnologia serve à manutenção e à otimização do poder vigente. A convergência entre o imperativo econômico e a necessidade estatal de regulação populacional resultou na cimentação de um capitalismo de vigilância (Zuboff, 2018). Essa simbiose resultou na constituição de uma sociedade de vigilância, caracterizada pelo monitoramento constante e pela vigília invisível sobre a vida das pessoas (Rodotà, 2008).

O ponto mais avançado dessa evolução reside na capacidade de predição e classificação de comportamentos. A passagem dos gestos punitivos para a gerência difusa e informatizada de comportamentos (Duarte; Nunes; Lima, 2023) culminou em uma governamentalidade algorítmica, que busca antecipar e prevenir eventos com fundamento em critérios de normalidade ou anormalidade (Rouvroy; Berns, 2010).

O desenvolvimento e a crescente adoção de tecnologias de reconhecimento facial exemplificam de forma mais contundente a materialização contemporânea da sociedade de

de previsões subsequentes, fenômeno que O'Neil (2017) denomina *feedback loop*, cuja análise será feita posteriormente.

controle e do policiamento preditivo (Duarte; Nunes; Lima, 2023). Ao converter características biométricas em insumos de dados quantificáveis e processáveis em tempo real, essas tecnologias representam o ponto nevrálgico onde o capitalismo de dados, a lógica do risco securitário e a governamentalidade algorítmica convergem para impor um novo patamar de dominação social, fundado na identificação instantânea e na classificação imediata de populações (Duarte; Nunes; Lima, 2023).

3 A “CAIXA-PRETA” DO RACISMO: OPACIDADE ALGORÍTMICA, VIESES COGNITIVOS E A REPRODUÇÃO DE HIERARQUIAS RACIAIS

O percurso desenvolvido no capítulo anterior evidenciou uma racionalidade de controle fundada na vigilância difusa, na datificação da vida social e na gestão antecipatória do risco. A partir desse enquadramento, o presente capítulo desloca o foco da macroestrutura sociopolítica para a engrenagem técnica que sustenta essas dinâmicas, examinando os fundamentos conceituais, epistemológicos e jurídicos dos dispositivos tecnológicos de monitoramento.

Inicialmente, esclarece-se a distinção entre algoritmos simples, baseados em sequências lineares de instruções, e modelos complexos, que fazem uso de grandes volumes de dados. Nesse contexto, introduzem-se as noções de *big data* e *big analytics* como vetores da expansão de sistemas automatizados.

Em seguida, o capítulo delimita o conceito de inteligência artificial, abordando suas principais correntes teóricas e fixando o paradigma da inteligência artificial estreita como referência analítica desta pesquisa.

Ao recuperar o debate entre sintaxe e semântica a partir da formulação de Searle (2006), o texto estabelece que sistemas algorítmicos são incapazes de apreender o significado dos símbolos que manipulam. Essa delimitação fornece o suporte necessário para compreender a natureza das decisões automatizadas e de suas implicações sociais.

A etapa seguinte concentra-se na incorporação de vieses e heurísticas aos sistemas computacionais. O exame demonstra que distorções cognitivas presentes na experiência humana são transpostas para o plano tecnológico por meio da seleção de variáveis, da definição de métricas e da composição das bases de treinamento. A discussão ganha concretude com a referência às disparidades identificadas em tecnologias de reconhecimento facial, cujas taxas de erro variam significativamente conforme gênero e raça.

A partir dessa constatação, o capítulo aprofunda a noção de racismo algorítmico como o processo pelo qual hierarquias raciais são absorvidas por modelos estatísticos e reorganizadas na lógica da decisão automatizada. O estudo dialoga com a formulação do dispositivo de racialidade e com a ideia de contrato racial, situando a tecnologia no interior de uma formação social que privilegia grupos hegemônicos.

Na sequência, o texto aborda a opacidade algorítmica como fenômeno multidimensional que dificulta a compreensão, auditoria e contestação das decisões automatizadas. São examinadas suas dimensões intrínseca, estratégica e cognitiva, bem como seus reflexos sobre a ordem constitucional. A análise demonstra que a opacidade impacta diretamente a legitimidade das providências estatais mediadas por sistemas inteligentes.

O capítulo encerra-se com a problematização da responsabilidade sobre as decisões tomadas pelas máquinas. Partindo da premissa de que a responsabilização pressupõe consciência e intencionalidade, sustenta-se que o olhar jurídico deve recair sobre os agentes humanos envolvidos na concepção, implementação e utilização dos sistemas algorítmicos.

Com esse arcabouço estabelecido, o capítulo inicia-se pela delimitação conceitual do algoritmo e de sua racionalidade classificatória, base indispensável para toda a crítica subsequente.

3.1 Algoritmos: do modelo simples ao aprendizado de máquina

A compreensão do que define um algoritmo é tema de intenso debate acadêmico (Beer, 2017; Gurevich, 2012; Moschovakis, 2001). Em termos gerais, contudo, há convergência quanto ao seu núcleo estrutural: o algoritmo consiste em um procedimento matemático, estruturado em sequências finitas e ordenadas, destinado ao fornecimento de diretrizes a sistemas computacionais para a execução de tarefas previamente estabelecidas (Oliveira, 2020, p. 41; Domingos, 2017a, p. 25).

Beer (2017, p. 5-6) argumenta que essa definição não deve ser lida isoladamente, visto que o algoritmo não é um objeto autônomo, existente fora de uma “ecologia social”. Tratá-lo dessa maneira seria insuficiente para captar sua real dimensão, uma vez que esses mecanismos não funcionam em um vácuo sociopolítico. Para o autor, a criação, a implementação prática e as constantes atualizações (*redesigns*) dos algoritmos são elementos indissociáveis do contexto social, moldados por pressões externas e objetivos de grupos humanos específicos.

Do ponto de vista operacional, a finalidade precípua de uma estrutura algorítmica consiste na decodificação de padrões complexos por meio do processamento sistemático de dados (Searle, 2006; Corrêa, 2021; O’Neil, 2017; Machado Segundo, 2023; Zuboff, 2018). Para que essa operação ocorra, o sistema depende de um fluxo inicial de informações, designadas

entradas (*inputs*) – que compreendem as variáveis brutas fornecidas ao sistema. Esse aporte informacional é submetido a um processo de triagem, no qual os dados são filtrados, organizados e categorizados, com o objetivo de traduzir a realidade empírica em elementos quantificáveis (Searle, 2006; Domingos, 2017a).

O encerramento desse ciclo resulta nos *outputs*, ou saídas, que correspondem ao produto final das operações realizadas, podendo manifestar-se, por exemplo, na resolução de problemas ou na automação de decisões (Domingos, 2017a; Kleinberg *et al.*, 2018; Machado Segundo, 2023, p. 31). Os algoritmos estruturados sob essa lógica linear e rígida são considerados simples (Domingos, 2017b; Crestane; Leal, 2024), caracterizando-se por uma previsibilidade que não admite variações além do que foi explicitamente codificado.

Em um plano de maior sofisticação, o avanço da tecnologia permitiu o desenvolvimento de algoritmos complexos, fundamentados em princípios de inteligência artificial, os quais se distinguem por sua capacidade de autoprogramação (Kleinberg *et al.*, 2018; Utset, 2021). Nesses modelos, o programador, em que pese seja o responsável por definir o objetivo da tarefa e fornecer os dados iniciais¹³ (Kleinberg *et al.*, 2018, p. 136), possui atuação limitada. Isso porque ele concede ao sistema a autonomia necessária para traçar os caminhos lógicos que levam à solução mais eficaz (Domingos, 2017a, p. 31; Russell; Norvig, 2010, p. 39), de modo que o algoritmo passa a operar por inferência (Domingos, 2017a; Russell; Norvig, 2010).

A expansão desse paradigma relaciona-se ao crescimento do *big data*,¹⁴ expressão que designa a coleta, o gerenciamento e o tratamento de grandes volumes de dados (Frazão, 2020; Téllez Carvajal, 2020, p. 156). A magnitude quantitativa dessas informações, sua heterogeneidade e a necessidade de processamento em tempo reduzido constituem um ambiente propício à aplicação de técnicas estatísticas avançadas.

¹³ Denominados “dados de treinamento” (*training data*), esse conjunto de informações é introduzido diretamente no sistema algorítmico. A partir deles, o programa identifica padrões estatísticos relevantes de forma autônoma (Kleinberg *et al.*, 2018, p. 136; Utset, 2021, p. 167-168).

¹⁴ Cinco características fundamentais, conhecidas como “5Vs”, diferenciam o *big data* dos conjuntos de dados tradicionais: volume, variedade, velocidade, veracidade e valor (Hoffmann-Riem, 2022). O volume refere-se à quantidade massiva de dados gerados e registrados a cada segundo no ecossistema digital. A velocidade, por sua vez, diz respeito à agilidade com que esses dados são produzidos e precisam ser manipulados, muitas vezes exigindo análises em tempo real para serem considerados úteis. A variedade reflete a heterogeneidade das fontes e dos formatos desses dados. A veracidade é o pilar que garante a confiabilidade, a qualidade e a precisão das informações tratadas. Finalmente, o valor representa o propósito estratégico de todo o sistema, responsável por transformar a massa de dados em conhecimento (Hoffmann-Riem, 2022, p. 19-20).

Nesse contexto emerge o *big analytics*, conjunto de métodos empregados para examinar volumosas bases de dados com o objetivo de identificar padrões, antecipar tendências comportamentais e apoiar a tomada de decisões estratégicas (Frazão, 2019; 2020; Hoffmann-Riem, 2020, p. 2). Entre as técnicas associadas a esse ambiente, destaca-se o aprendizado de máquina (*machine learning*), considerado um dos principais subconjuntos da inteligência artificial (Corrêa, 2021; Crestane; Leal, 2024; Kaufman, 2020).

No *machine learning*, o sistema realiza ajustes contínuos em seus parâmetros a partir da exposição a grandes conjuntos de dados, sendo capaz de prever e reagir a diferentes cenários sem uma programação específica para cada situação (Corrêa, 2021, p. 192-193; Kaufman, 2020, p. 67628). Isso ocorre porque o *software* identifica regularidades e produz inferências que orientam respostas a novas entradas informacionais (Corrêa, 2021, p. 192-193). Segundo Corrêa (2021, p. 193), trata-se de um termo “guarda-chuva”, que acolhe diversas metodologias de ensino computacional, como o *deep learning*, visando dotar a máquina de uma capacidade de adaptação que mimetiza (Searle, 2006) processos de aprendizagem observados na natureza.

O aprendizado profundo (*deep learning*), subárea do *machine learning*, é um desdobramento técnico dessa lógica (Corrêa, 2021; Kaufman, 2020; Hoffmann-Riem, 2020). Esse modelo é baseado em redes neurais artificiais¹⁵ compostas por múltiplas camadas de processamento, nas quais se organizam unidades computacionais denominadas neurônios (Hoffmann-Riem, 2020; Kaufman, 2020). A profundidade dessas redes permite ao *deep learning* expandir seu próprio código sem a necessidade de intervenção humana, por meio da extração automática de características complexas presentes em imagens, textos e áudios (Hoffmann-Riem, 2020).

Consoante exposto na seção seguinte, tal arquitetura constitui o fundamento de diversas aplicações inteligentes, entre elas as tecnologias de reconhecimento facial, cuja operação depende da extração e comparação automatizada de características biométricas presentes em imagens digitais (Corrêa, 2021; Kaufman, 2020).

¹⁵ Redes neurais são modelos computacionais de aprendizado de máquina, projetadas para identificar padrões em grandes volumes de dados (Kaufman, 2020, p. 67626-67627). Elas são compostas por neurônios, isto é, unidades de processamento de informação que se organizam em camadas: as de entrada (que recebem os dados brutos), as ocultas (onde ocorre o processamento das informações) e as de saída (onde o resultado final é produzido).

3.2 Os limites da cognição artificial

O desenvolvimento dos algoritmos descrito no tópico anterior conduz ao domínio da inteligência artificial. Inserida no campo da ciência da computação, a inteligência artificial compõe área dedicada à criação de sistemas capazes de desempenhar tarefas associadas à cognição humana, como o reconhecimento de padrões, a formulação de previsões, a classificação de informações e a tomada de decisões (Domingos, 2017a; Russell; Norvig, 2010).

Desde sua consolidação na década de 1950, sob a influência de pesquisadores como Turing e McCarthy, o campo passou a reunir distintas correntes teóricas interessadas em compreender de que maneira processos de raciocínio poderiam ser descritos formalmente e, assim, reproduzidos em linguagem computacional (Corrêa, 2021; Kaufman, 2020; Oliveira, 2020). Conforme sintetizam Russell e Norvig (2010), parte dos estudiosos caracteriza como inteligente o algoritmo capaz de mimetizar o pensamento ou o comportamento humano observável. Outra vertente, contudo, privilegia a racionalidade orientada ao cumprimento eficiente de objetivos previamente definidos.

Sem a pretensão de exaurir as diversas acepções doutrinárias¹⁶¹⁷ do tema, é válido discutir brevemente duas visões que moldaram o campo da inteligência artificial. McCarthy

¹⁶ Hofstadter e Sander (2013) desenvolvem outra perspectiva relevante para a compreensão da inteligência artificial. Em *Surfaces and Essences: Analogy as the Fuel and Fire of Thinking*, os autores propõem que a analogia é o núcleo de todo o intelecto humano. Nessa acepção, o pensamento consiste em um processo ininterrupto de comparações que conferem sentido à realidade, viabilizando o reconhecimento de padrões e a construção de novos significados. A analogia, nesse sentido, é o vetor que sustenta tanto a linguagem quanto a inventividade humana, ao unir diferentes domínios da experiência. A inteligência manifesta-se, então, por intermédio da fluidez conceitual (*conceptual slippage*), faculdade que permite a expansão e a adaptação das categorias mentais diante de cenários distintos. Malgrado não seja um tratado sobre inteligência artificial, a obra discute como a aptidão analógica é fundamental para a cognição e, por conseguinte, para aferir a natureza de um sistema inteligente. Para os autores, as tecnologias contemporâneas estão confinadas ao domínio das superfícies, isto é, aos aspectos imediatos e literais de determinado objeto, conceito ou situação. O que hoje se celebra como inteligência é, em grande medida, um mimetismo fundamentado em correlações estatísticas, uma vez que os sistemas tecnológicos são incapazes de acessar o núcleo abstrato, ou a essência, que permite ao cérebro criar e processar analogias. Em última análise, uma máquina somente poderia ser verdadeiramente inteligente se fosse capaz de, assim como os humanos, conceber analogias de forma espontânea.

¹⁷ Larson (2021), em suas investigações sobre a natureza da mente e da tecnologia, argumenta que a ideia de que máquinas alcançarão inevitavelmente a inteligência humana ou a superinteligência é um mito. O autor descreve o intelecto humano como um conjunto de operações cognitivas centradas na abdução, processo pelo qual agentes formulam hipóteses explicativas a partir de evidências parciais e contextos amplos. De acordo com essa perspectiva, a inteligência é a capacidade de formular explicações plausíveis diante de nuances e informações fragmentadas, um processo que ocorre por meio de saltos intuitivos. Essa faculdade abdutiva é o que confere ao pensamento humano a capacidade de navegar pela ambiguidade do mundo real e que o distingue da tecnologia. Segundo Larson (2021), ao contrário da mente humana, o desenvolvimento tecnológico é conduzido pela lógica indutiva e dedutiva. Por essa razão, ainda que os sistemas contemporâneos operem com maestria na identificação de padrões em vastos conjuntos de dados, eles não são capazes de “saltar” para uma compreensão abdutiva típica da humanidade.

(2000), precursor da expressão “inteligência artificial”, partiu da premissa de que funções intelectuais poderiam ser descritas com precisão suficiente para serem implementadas em máquinas (Corrêa, 2021, p. 189-190; Russell; Norvig, 2010). A inteligência, nesse sentido, consistiria em um conjunto estruturado de procedimentos suscetíveis de formalização lógica.

Searle (2006), por outro lado, propôs uma distinção fundamental entre dois modelos teóricos: a Inteligência Artificial Estreita (*Artificial Narrow Intelligence*), também conhecida como “IA fraca”, e a Inteligência Artificial Geral (*Artificial General Intelligence*), ou “IA forte”. Na primeira espécie, o computador limita-se a simular processos mentais sem de fato possuí-los, isto é, a executar tarefas específicas por meio da manipulação formal de símbolos, alcançando desempenho eficaz em domínios delimitados. Nesta categoria, não se atribui ao *hardware* ou ao *software* qualquer forma de percepção, subjetividade ou entendimento real sobre as informações processadas (Oliveira, 2020, p. 41).

Na segunda modalidade, por outro lado, admite-se a possibilidade de que um sistema computacional desenvolva consciência e intencionalidade autênticas, desde que adequadamente programado (Oliveira, 2020). Na IA forte, a inteligência e a subjetividade seriam um fenômeno estritamente técnico, de modo que a implementação de algoritmos de complexidade suficiente poderia resultar na emergência de estados mentais análogos aos humanos (Oliveira, 2020, p. 42).

Para contestar a premissa da IA forte, Searle (2006) formulou o experimento do Quarto Chinês.¹⁸ Nesse exercício teórico, o filósofo recorreu à dicotomia entre sintaxe e semântica¹⁹ para demonstrar que a mera aplicação de regras formais não equivale à apreensão

¹⁸ Na metáfora, um indivíduo que desconhece a língua chinesa é isolado em um recinto e instruído a responder a perguntas enviadas por falantes nativos. Com o auxílio de um manual de instruções escrito em seu idioma materno, o sujeito consegue fornecer respostas corretas apenas correlacionando determinados símbolos. Para um observador externo, a precisão das respostas leva a crer que o indivíduo compreende o idioma de forma genuína. Contudo, o confinado apenas executa um procedimento mecânico, sem intencionalidade ou consciência real sobre os ideogramas (Searle, 2006). Não se desconhecem as críticas ao argumento do Quarto Chinês, todavia, foge do escopo do presente trabalho enumerá-las, bem como rechaçá-las. Para tanto, ver: HAUSER, Larry. Replies and Rejoinders. In: HAUSER, Larry. **Chinese Room Argument**. [S. l.]: Internet Encyclopedia of Philosophy, [s.d.]. Disponível em: <https://iep.utm.edu/chinese-room-argument/#H2>. Acesso em: 10 maio 2026.

¹⁹ A distinção é essencial para compreender por qual motivo os algoritmos de reconhecimento facial, apesar de sua precisão técnica, são suscetíveis a erros e preconceitos: eles carecem da percepção semântica da realidade, operando em um vácuo de significado que os torna dependentes da integridade e da ética das bases de dados com as quais foram alimentados (Duarte; Nunes; Lima, 2023; Martins *et al.*, 2024; Silva, 2024). Enquanto um ser humano interpreta um rosto por meio de uma rede complexa de significados culturais, afetivos e históricos, a inteligência artificial decompõe essa imagem em vetores numéricos e probabilidades estatísticas. Nesta pesquisa, defende-se que os riscos de discriminação surgem do descompasso entre a lógica formal e a complexidade da experiência humana. Sustenta-se, então, que a falha recorrente na identificação de determinados grupos sociais é

de significados (Oliveira, 2020). Enquanto a sintaxe corresponde ao encadeamento formal de símbolos segundo regras estruturadas, como a gramática ou o código binário, a semântica envolve a interpretação de determinado signo.

Nesse sentido, um computador, ainda que sofisticado, atua exclusivamente no nível sintático – conquanto simule uma faculdade linguística, não compreende de forma autêntica o sentido das expressões que manipula. A IA forte seria, portanto, uma impossibilidade lógica, que apenas mimetiza a mente humana mediante parâmetros pré-estabelecidos de *inputs* e *outputs* (Searle, 2006, p. 90). No entanto, a execução de um programa não seria capaz de gerar, por si só, a intencionalidade ou os estados mentais que caracterizam a consciência humana.

No presente trabalho, a inteligência artificial será compreendida como o conjunto de sistemas capazes de executar tarefas cognitivas específicas mediante aprendizado estatístico e modelagem matemática (Corrêa, 2021; Domingos, 2017a; Frazão, 2019; Hoffmann-Riem, 2020; Russell; Norvig, 2010). Adotar-se-á o paradigma da inteligência artificial fraca, em conformidade com as premissas estabelecidas por Searle (2006), uma vez que, no estágio atual, a inteligência artificial carece de consciência ou agência própria (Greco, 2020; Boeing; Rosa, 2020; Domingos, 2017a; Oliveira, 2020).

O aprofundamento dessa discussão requer, porém, examinar como decisões automatizadas incorporam distorções cognitivas presentes em suas bases informacionais de treinamento.

3.3 Vieses, heurísticas e a transposição de preconceitos ao *design* tecnológico

O uso da inteligência artificial é frequentemente associado à promessa de maior precisão diagnóstica e eficiência administrativa, haja vista que a ferramenta automatiza processos burocráticos antes dependentes de tempo e discricionariedade humana (Bioni, 2020; Pasquale, 2016; Duarte; Nunes; Lima, 2023; Martins *et al.*, 2024). De acordo com Han (2018, p. 78), o uso de *big data* tornou possível “uma forma de controle muito eficiente”, uma vez que “o pan-óptico digital oferece uma visão em 360° dos seus internos”. Nessa abordagem, a vigilância digital “é mais eficiente porque é aperspectivista” (Han, 2018, p. 78), o que possibilita o monitoramento contínuo do corpo social a partir de qualquer ângulo, eliminando

produto da incapacidade de apreensão da diversidade humana, muitas vezes em razão de um banco de dados enviesado (Oliveira, 2020).

pontos cegos.

Com base nesse discurso, a capacidade de classificação e predição impulsionou a incorporação de tecnologias digitais em ambientes institucionais, sobretudo no âmbito da segurança pública, facilitando a transição de um modelo de policiamento reativo para um modelo preventivo (Bruno, 2013; Oliveira, 2020; Nunes; Lima; Cruz, 2023; Pullen; Schefer, 2021; Duarte; Nunes; Lima, 2023; Martins *et al.*, 2024; Silva, 2024). Nesse contexto, a compreensão dos vieses torna-se indispensável para avaliar os efeitos sociais da mediação tecnológica.

Em termos gerais, vieses correspondem a distorções cognitivas no processamento de informações. Essas falhas frequentemente induzem o intérprete a erros sistemáticos de julgamento (Freitas, 2013, p. 225; Kahneman, 2012; Nunes; Lud; Pedron, 2018; Smith, 2019), uma vez que simplificam de maneira excessiva a realidade (Tonetto *et al.*, 2006, p. 187). Tais equívocos derivam de padrões de pensamento automáticos e não conscientes, resultando em desvios de racionalidade, interpretações ilógicas e julgamentos imprecisos (Tversky; Kahneman, 2012; Tonetto *et al.*, 2006).

A existência dos vieses fundamenta-se em processos evolutivos e biológicos orientados para a adaptação e a sobrevivência do organismo. Estudos mostram que o cérebro humano desenvolve estratégias para otimizar o processamento de informações em ambientes complexos e sobrecarregados de estímulos, a fim de evitar o desgaste energético exigido por um raciocínio lógico deliberativo (Horta, 2019; Kahneman, 2012; Tavares, 2021).

As heurísticas são expressões desses mecanismos. Elas representam atalhos mentais ou procedimentos simplificadores que permitem decisões rápidas diante da incerteza (Kahneman, 2012; Tonetto *et al.*, 2006; Nunes; Lud; Pedron, 2018; Fenoll, 2018). De acordo com Kahneman (2012, p. 127), o termo diz respeito a “um procedimento simples que ajuda a encontrar respostas adequadas, ainda que geralmente imperfeitas, para perguntas difíceis”. Por meio das heurísticas, é possível decidir “sem ter que considerar todas as informações relevantes, confiando, em vez disso, em um conjunto limitado de pistas” (Peer; Gamliel, 2013, p. 114).

A lógica que fundamenta esses processos evidencia que as decisões humanas são mediadas por filtros interpretativos socialmente²⁰ construídos (Brayne, 2021). Esses filtros

²⁰ Nesse sentido, Brayne (2021) argumenta que a distribuição assimétrica da capacidade de coletar dados e intervir em trajetórias individuais consolida disparidades na formulação de políticas públicas e no exercício do controle

estabelecem categorias e hierarquias a partir de simplificações ancoradas nas dinâmicas de poder da sociedade (Brayne, 2021, p. 18). Experiências históricas, valores culturais e narrativas coletivas influenciam a percepção do risco e a atribuição de significado a determinados comportamentos (Hilbert, 2012; Peer; Gamliel, 2013). O excesso de informações, por exemplo, pode resultar na valorização seletiva de dados que confirmam crenças pré-existentes, reforçando vieses cognitivos e sociais (Hilbert, 2012; Peer; Gamliel, 2013).

De modo semelhante, a construção de narrativas coerentes pode ser influenciada pelo preenchimento de lacunas com estereótipos e generalizações (Tonetto *et al.*, 2006), e a necessidade de agir rapidamente pode estar baseada em dados incompletos (Hilbert, 2012; Peer; Gamliel, 2013). Além disso, os limites da memória contribuem para que lembranças sejam reforçadas de forma tendenciosa, preservando apenas elementos que sustentam visões prévias de mundo (Kahneman, 2012).

A transposição de vieses do plano cognitivo para o tecnológico ocorre no âmbito dos *built-in biases* (vieses embutidos), quando sistemas automatizados apreendem e replicam valores, interesses e preconceitos humanos (Frazão, 2019, p. 39; Oliveira, 2020; Gilliom; Monahan, 2013). Esse fenômeno é influenciado pelo *mathwashing* (Polli, 2017) – a tendência de atribuir objetividade, infalibilidade e neutralidade à tecnologia –, conferindo legitimidade simbólica aos algoritmos, apesar de sua tendência à amoralidade (Kelleher; Tierney, 2018). Para Frazão (2019, p. 39), é comum que a programação de sistemas automatizados esteja “permeada de vieses e preconceitos dos programadores, intencionais ou não, que podem levar a erros de diagnóstico ou a graves discriminações”.

social. Conforme sintetiza a autora, “Algoritmos não transcendem o social, mas são moldados pelo mundo social em que são criados e utilizados. As atividades que geram e as tecnologias que analisam dados estão todas inseridas em contextos sociais e estruturas de poder, de modo que os dados resultantes são tudo menos ‘naturais’, desconectados ou puramente descritivos. Pelo contrário, são as pessoas situadas em contextos sociais, organizacionais e institucionais preexistentes que decidem quais dados coletar e analisar, sobre quem e com que finalidade. Assim, tal como os indivíduos carregam uma série de vieses implícitos que afetam as suas decisões, os algoritmos estão carregados com uma estrutura de preconceitos implícitos que afetam os dados que analisam e produzem. O que os dados podem medir e quantificar não é uma questão técnica, mas sim normativa, relacionada a prioridades institucionais, imperativos organizacionais e preferências individuais e coletivas” (Brayne, 2021, p. 18, tradução nossa). No original: “*Algorithms do not transcend the social, but are shaped by the social world in which they are created and used. The activities that generate and the technologies that analyze data are all embedded within social contexts and power structures, so the resulting data are anything but ‘natural’, detached, or purely descriptive. Rather, people situated in preexisting social, organizational, and institutional contexts decide what data to collect and analyze, about whom, and for what purpose. So, just as individuals carry a range of implicit biases that affect their decisions, algorithms are loaded up with a scaffolding of implicit biases affecting the data they analyze and produce. What data can measure and quantify is not a technical question, but a normative one related to institutional priorities, organizational imperatives, and individual and group preferences*”.

Essa inserção de vieses ocorre por duas vias principais: a seleção de variáveis no *design* do sistema e a composição das bases de dados utilizadas para treinamento (Corrêa, 2021; Kaufman, 2020; Benjamin, 2019). Primeiro, desenvolvedores estabelecem critérios de relevância, métricas de desempenho e parâmetros de validação de acordo com suas subjetividades. Desse modo, a escolha das variáveis define quais dimensões da realidade serão mensuradas e quais permanecerão invisíveis. Então, os dados que alimentam os algoritmos de aprendizado de máquina e aprendizado profundo refletem padrões históricos de discriminação (Corrêa, 2021; Kaufman, 2020; Silva, 2024).

Nesse sentido, bases incompletas, desproporcionais, imprecisas ou concentradas em determinados grupos conduzem a inferências igualmente distorcidas. Redman (2018) ressalta que a qualidade dos dados históricos influencia diretamente o desempenho do modelo preditivo: dados de baixa qualidade podem prejudicar tanto o treinamento quanto a análise de novos dados, utilizados em previsões e decisões futuras. Como consequência, “os algoritmos podem perpetuar injustiças, preconceitos e discriminações” (Frazão, 2019, p. 39).

Segundo Redman (2018), para treinar adequadamente um modelo preditivo, é necessário dispor de dados apropriados, isto é, de informações imparciais que cubram toda a gama de entradas para as quais se pretende desenvolver o modelo. Contudo, o autor explica que a maioria dos conjuntos de dados utilizados em sistemas de inteligência artificial contemporâneos não satisfaz os requisitos básicos de qualidade. As razões para essa deficiência variam desde processos lógicos excessivamente complexos e erros humanos até desenvolvedores que desconhecem as expectativas quanto à composição das bases informacionais, produzindo conjuntos pouco representativos ou incompletos (Oliveira, 2020; Redman, 2018).

Citam-se, a título ilustrativo, as tecnologias de reconhecimento facial desenvolvidas em países ocidentais, que, não raro, agem sobre acervos de dados compostos majoritariamente por imagens de homens brancos,²¹ com pouca ou nenhuma representação de grupos segregados (Oliveira, 2020, p. 43). Buolamwini e Gebru (2018) evidenciam disparidades substanciais na precisão dessas ferramentas, especialmente em relação a pessoas de pele escura. Enquanto a acurácia é quase absoluta para homens de pele clara, as taxas de erro para mulheres negras oscilam entre 61% e 72,4% (Buolamwini; Gebru, 2018, p. 10), resultando em identificações

²¹ Buolamwini e Gebru (2018) classificam essas informações como *pale male data*, expressão que se refere aos conjuntos de dados excludentes, nos quais não há representatividade de gêneros e tons de pele.

equivocadas e prisões injustas. As autoras denominam esse viés incorporado nas tecnologias biométricas de olhar codificado (*coded gaze*), conceito que descreve a reprodução e amplificação algorítmica de falhas no reconhecimento de minorias (Buolamwini; Gebru, 2018).

Na mesma linha de raciocínio, Noble (2018) rejeita a neutralidade algorítmica, argumentando que as decisões automatizadas estruturam o conhecimento e criam realidades materiais que marginalizam grupos vulneráveis. A autora cunha o termo “opressão algorítmica” para descrever como os algoritmos privilegiam a branquitude e reproduzem estereótipos sexistas e racistas: resultados de busca, por exemplo, podem priorizar conteúdos que reforçam imagens discriminatórias, invisibilizar vozes subalternizadas e normalizar narrativas que legitimam desigualdades.

No ambiente jurídico, essas dinâmicas atingem garantias fundamentais como a presunção de inocência e o devido processo legal (Neira Pena, 2021; Roa Avella; Sanabria-Moyano; Dinas-Hurtado, 2022), analisados em momento posterior deste capítulo. De outra sorte, no âmbito da segurança pública, essa dinâmica manifesta-se com maior relevância no policiamento preditivo e nos *softwares* de reconhecimento facial (Gilliom; Monahan, 2013).

Ao utilizarem dados históricos para prever a criminalidade, tais sistemas frequentemente concentram o patrulhamento em territórios e grupos sociais vulnerabilizados (Silva, 2024), ao passo que negligenciam crimes em áreas privilegiadas (Firmino, 2018; O’Neil, 2017). Nesse sentido, Lum e Isaac (2016) demonstram que o aumento da vigilância em bairros periféricos e racializados, como consequência do policiamento preditivo, gera novos registros. Estes, por sua vez, confirmam os padrões anteriores, em um ciclo de retroalimentação destrutivo, validando e intensificando o viés territorial e racial original.

A discussão conduzida até este ponto evidencia que os sistemas de inteligência artificial incorporam padrões de classificação extraídos de contextos sociais e subjetivos concretos. No tópico subsequente, serão examinadas as razões pelas quais vieses de caráter racial, quando assimilados por modelos algorítmicos, influenciam a distribuição institucional da vigilância, da suspeição e do controle.

3.4 O racismo algorítmico como um dispositivo tecnológico de racialidade

Quando as realidades sociais que alimentam sistemas algorítmicos são atravessadas por desigualdades raciais, a mediação tecnológica tende a absorver essas distorções e a

reinscrevê-las na racionalidade computacional (Duarte; Nunes; Lima, 2023; Martins *et al.*, 2024; Silva, 2024). Por essa razão, o estudo do racismo no ambiente digital exige o retorno às bases que o estruturam como mecanismo de organização das hierarquias sociais brasileiras.

O racismo, conforme formulado por Almeida (2019) e Moreira (2020), diz respeito a um sistema de dominação que organiza e condiciona as relações sociais, econômicas, políticas e jurídicas. Mais do que meras manifestações individuais, trata-se de um componente estruturante do tecido social, cuja função se concentra no estabelecimento de estratos fundamentados no conceito de raça, o que assegura privilégios aos grupos hegemônicos em detrimento de coletividades marginalizadas.

No centro dessa arquitetura localiza-se o que Carneiro (2023) denomina dispositivo de racialidade, um instrumento de dimensões ontológicas, epistemológicas e políticas. Inspirada na noção foucaultiana de dispositivo, mas adaptada às especificidades de uma sociedade multirracial de herança escravocrata, a autora descreve uma rede heterogênea composta por discursos, instituições, normas, saberes e modos de subjetivação direcionados à manutenção da subalternidade da população negra. O dispositivo de racialidade posiciona o sujeito racializado, identificado como o “Outro”, na categoria de um “não ser”.²² De maneira simultânea, esse mecanismo consolida a branquitude como um “ser” universal – o corpo branco é, nesse sentido, a referência última de humanidade, racionalidade e intelectualidade, valores negados aos grupos racializados, frequentemente relegados à condição de “selvageria”.

A sustentação desse arranjo decorre de processos históricos de epistemicídio e da vigência de um contrato racial²³ (Carneiro, 2023; Mills, 1997) que assegura a supremacia da branquitude (Bento, 2022). Esse acordo organiza a coletividade a partir de distinções implícitas que restringem o reconhecimento social ao grupo hegemônico e distribuem direitos, oportunidades e proteção institucional de maneira desigual entre indivíduos negros e brancos (Mills, 1997). Essa dinâmica preserva o monopólio branco sobre recursos econômicos, políticos e intelectuais, ao passo que limita o acesso de sujeitos racializados aos espaços de poder,

²² A “zona do não ser” é um conceito herdado de Fanon (2008). Na obra *Pele negra, máscaras brancas*, o autor descreve um espaço social e ontológico de aniquilação subjetiva do colonizado, particularmente o negro. Nessa área de não-humanização, a identidade é negada ao corpo racializado, que é tratado como um objeto ou uma antítese à pele branca e impedido de construir sua própria subjetividade.

²³ De acordo com a teoria crítica do contrato racial, formulada por Mills (1997), a estrutura política e moral da sociedade moderna está fundamentada em um acordo tácito de dominação branca que legitima a subordinação de grupos não brancos. Em contraste com as concepções clássicas de contrato social, que pressupõem cooperação universal e igualitária, o contrato racial institui uma hierarquia que privilegia a branquitude, relegando as populações racializadas a um estado permanente de exploração, exclusão e desumanização.

produção de conhecimento e exercício pleno da cidadania (Carneiro, 2023).

O pacto narcísico da branquitude é uma dimensão complementar dessa conjuntura (Bento, 2022). Trata-se de um acordo implícito de autopreservação, que garante privilégios intragrupais a pessoas brancas por meio da naturalização de sua própria centralidade. Bento (2022) postula que a branquitude se apresenta como sujeito neutro e universal, ocultando sua participação ativa na reprodução das desigualdades sociais. Com isso, os interesses do grupo dominante são resguardados, enquanto seus integrantes permanecem alheios à responsabilidade pela perpetuação da discriminação racial. Esse pacto manifesta-se na ocupação majoritária de espaços de poder, incluindo o campo da produção tecnológica e da formulação de políticas públicas relacionadas à inteligência artificial, áreas nas quais a baixa diversidade racial favorece a continuidade de padrões excludentes (Silva, 2024).

No plano digital, Silva (2024) compreende o racismo algorítmico como a face tecnológica desse projeto colonial. O autor emprega o conceito para descrever o processo acrítico pelo qual tecnologias, quando inseridas em contextos moldados pelo privilégio branco, reproduzem e reorganizam determinadas hierarquias sociais. Para ele, a algoritmização do racismo corresponde à “ordenação algorítmica de classificação social, recursos e violência em detrimento de grupos minorizados” (Silva, 2024, p. 66). Trata-se, ainda, de uma “camada adicional do racismo estrutural, que, além do mais, molda o futuro e os horizontes de relações de poder, adicionando mais opacidade sobre a exploração e a opressão global que já ocorriam desde o projeto colonial do século XVI” (Silva, 2024, p. 66). Segundo o pesquisador, essa dinâmica ganha concretude quando sistemas de decisão automatizada, supostamente neutros, empregam dados atravessados pela seletividade racial para embasar decisões igualmente enviesadas.

Todavia, essa problemática estende-se para além do uso de acervos de dados enviesados. Ao propor o conceito de *New Jim Code*,²⁴ Benjamin (2019) evidencia um conjunto de práticas que dão continuidade a mecanismos históricos de controle racial, agora inscritos no

²⁴ A expressão constitui um jogo de palavras com as *Leis de Jim Crow*, regime de segregação racial que vigorou no sul dos Estados Unidos até meados da década de 1960. Benjamin (2019) estabelece esse paralelo para ilustrar que, assim como o antigo regime segregacionista utilizava a lei para isolar e marginalizar corpos negros, o *New Jim Code* utiliza algoritmos e *softwares* de inteligência artificial para exercer funções semelhantes, atuando como ferramentas de controle social. A distinção fundamental entre os dois contextos reside na natureza da operação: enquanto o *Jim Crow* se manifestava de modo explícito, inscrito na legislação e em locais públicos, o *New Jim Code* funciona de maneira implícita, apresentando decisões discriminatórias como meros resultados matemáticos, o que torna a resistência política e jurídica ainda mais complexa.

próprio *design* de sistemas automatizados. Na perspectiva da autora, o risco dessa questão reside na aptidão de tecnologias digitais em projetar hierarquias raciais enquanto preservam uma aparência de neutralidade e objetividade. A socióloga observa que, diferentemente das leis de segregação vigentes na sociedade estadunidense do século XX – transparentes em sua violência –, os algoritmos funcionam de maneira opaca. Esse caráter implícito torna o racismo algorítmico ainda mais insidioso do que suas formas anteriores, o que dificulta sua identificação e contestação.

Nesse enquadramento, e em conformidade com as premissas estabelecidas por Bento (2022), o fenômeno encontra esteio em uma epistemologia da ignorância (Mills, 1997; Silva, 2024) – definida como a recusa ativa em reconhecer o papel da raça na conformação das disparidades sociais. No cenário tecnológico, essa pretensa neutralidade da branquitude, quando transposta para os códigos, culmina em algoritmos que negligenciam a interferência da raça em seu *design* e nas decisões por eles tomadas (Silva, 2024).

Um exemplo dessa cumplicidade não verbalizada entre pessoas brancas e sistemas inteligentes é o já mencionado *coded gaze* (Buolamwini; Gebru, 2018). Nele, a ausência de representatividade negra na composição das equipes de desenvolvimento, somada à baixa diversidade fenotípica nos dados de treinamento de inteligências artificiais, molda a forma como a máquina identifica e diferencia sujeitos sub-representados. O resultado é uma tecnologia que não reconhece a humanidade de sujeitos não brancos, tratando-os como anomalias ou erros de processamento (Buolamwini; Gebru, 2018).

No reconhecimento facial, características biométricas são convertidas em vetores numéricos, a partir dos quais modelos estatísticos realizam comparações e classificações identitárias (Souza; Zanatta, 2021). Como as bases de treinamento que reúnem esses dados são formadas predominantemente por rostos masculinos e de pele clara, o desempenho do sistema é comprometido (Buolamwini; Gebru, 2018). Estudos conduzidos pelo *National Institute of Standards and Technology* (NIST) revelam que tais tecnologias apresentam índices de falha significativamente superiores em relação a determinados grupos populacionais: os erros podem ser de dez a cem vezes mais frequentes entre indivíduos negros, indígenas e asiáticos (Grother; Ngan; Hanaoka, 2019; Nunes *et al.*, 2025, p. 5).

No Brasil, as tentativas de quantificar e reduzir identidades a códigos matemáticos intensificam práticas discriminatórias porque incidem sobre uma sociedade historicamente

balizada pela denegação do racismo. Gonzalez (2020) interpreta essa dinâmica como expressão de uma neurose cultural brasileira, fenômeno no qual a violência racial é reinterpretada por narrativas de harmonia social que visam deslegitimar a centralidade da raça na gênese das desigualdades. Em oposição a esses mitos, investigações contemporâneas (Reis *et al.*, 2021; Duarte; Nunes; Lima, 2023; Martins *et al.*, 2024) demonstram que, no país, mais da metade das intervenções policiais baseadas em biometria facial decorreu de falsos positivos (Nunes *et al.*, 2025, p. 5). Assim, como adverte Silva (2024), o racismo algorítmico potencializa o risco de detenções arbitrárias e o agravamento de discriminações no sistema de justiça nacional.

A algoritmização do racismo, portanto, expõe uma dupla opacidade: por um lado, nega a existência do racismo estrutural; por outro, sustenta a suposta neutralidade da tecnologia (Silva, 2024). A compreensão desse quadro permite examinar, no tópico seguinte, como a opacidade dos sistemas automatizados dificulta a identificação de assimetrias e limita a possibilidade de agência frente às decisões produzidas por modelos algorítmicos.

3.5 Democracia e opacidade algorítmica: tensões entre a “caixa-preta” e as garantias constitucionais

Pasquale (2016) recorre à metáfora da “caixa-preta” para descrever sistemas cujo funcionamento interno é inacessível ao escrutínio humano, sendo protegidos por barreiras informacionais e segredos comerciais. Sob esse enfoque, a opacidade algorítmica designa o conjunto de obstáculos que impossibilita a plena compreensão, auditoria e contestação das decisões produzidas por sistemas automatizados (Burrell, 2016). Trata-se de fenômeno multidimensional que abrange aspectos técnicos, institucionais e políticos, inerente aos modelos de aprendizado de máquina (Corrêa, 2021) que orientam a inteligência artificial contemporânea.

Em sua análise, Burrell (2016) postula que a carência de explicação inteligível acerca da trajetória entre os dados de entrada e de saída de um algoritmo possui três dimensões: a intrínseca, a intencional e a institucional. A primeira e mais enigmática forma é a opacidade intrínseca, típica dos modelos de aprendizado de máquina profundo (Corrêa, 2021). Essa modalidade decorre da complexidade técnica dos modelos computacionais contemporâneos, nos quais a lógica da decisão é produto de milhões de parâmetros e interações não lineares distribuídos em camadas de neurônios artificiais (Burrell, 2016).

A sofisticação dessa arquitetura excede a capacidade de visualização e o raciocínio

causal do cérebro humano, dificultando a reconstrução sequencial do percurso decisório, até mesmo por especialistas (Burrell, 2016; Rudin, 2019; Nunes; Marques, 2018, p. 8). Na primeira dimensão, a opacidade ocorre porque o sistema não utiliza conceitos semânticos humanos (Searle, 2006) para tomar decisões, mas sim valores numéricos abstratos que representam probabilidades estatísticas, os quais, aliados à alta dimensionalidade de dados, criam interdependências impossíveis de rastrear manualmente (Burrell, 2016).

De outra sorte, o enfoque intencional vincula-se às escolhas estratégicas voltadas à proteção jurídica e econômica. A opacidade é articulada por corporações e Estados para salvaguardar vantagens competitivas no mercado ou impedir a manipulação de sistemas por agentes externos. Segredos industriais e direitos de propriedade intelectual são mobilizados como justificativa para restringir o acesso ao código-fonte e aos dados de treinamento das tecnologias (Burrell, 2016; Rudin, 2019). Essa forma de ocultamento é, portanto, uma estratégia de poder que limita a auditoria social e permite que determinados atores se evadam da responsabilização pública.

Por seu turno, a terceira dimensão refere-se ao analfabetismo técnico ou à disparidade de competências (Burrell, 2016; Rudin, 2019). A sofisticação da ciência de dados, das linguagens de programação e do cálculo estatístico exige um grau de especialização que torna o funcionamento dos algoritmos inacessível para a vasta maioria da população²⁵ (Burrell, 2016; Rudin, 2019). Essa barreira cognitiva compromete a autonomia individual e o exercício pleno do contraditório mesmo na presença de acesso formal ao código-fonte, dada a dificuldade de traduzir a linguagem técnica em conceitos jurídicos ou sociais inteligíveis (Silva, 2024).

No plano jurídico-constitucional, a opacidade algorítmica tensiona princípios como

²⁵ Essa inacessibilidade estende-se igualmente aos representantes políticos. Cita-se a título ilustrativo o depoimento de Mark Zuckerberg ao Senado estadunidense em 2018, por ocasião do polêmico episódio em torno das empresas Meta e Cambridge Analytica. A controvérsia envolveu a coleta e o uso indevido de dados de até 87 milhões de usuários do Facebook para fins de perfilamento político e publicidade eleitoral direcionada (Hinds; Williams; Joinson, 2020). Em sua declaração, Zuckerberg assumiu que a plataforma enfrentava problemas relacionados à privacidade e segurança, além de reconhecer que o acompanhamento dos fluxos de dados direcionados a terceiros foi insuficiente para impedir o uso nocivo de suas ferramentas. Durante a audiência, muitos senadores demonstraram dificuldade em compreender aspectos básicos do modelo de negócios da Meta, incluindo a monetização por publicidade, a coleta de dados e a lógica de direcionamento algorítmico (Kosoff, 2018). Essa assimetria informacional entre os senadores e a *big tech* impediu uma interpelação plenamente eficaz, uma vez que a sessão, em diversos momentos, assumiu feição explicativa ou pedagógica, em detrimento de uma postura fiscalizatória. O acontecimento evidencia como a mediação democrática sobre sistemas algorítmicos depende de competências técnicas que os agentes públicos nem sempre possuem. Observa-se, a partir disso, que as barreiras provenientes da opacidade não se restringem ao funcionamento dos algoritmos, mas alcançam também aqueles que detêm condições reais de exigir explicações, compreendê-las, traduzi-las juridicamente e convertê-las em instrumentos de responsabilização.

publicidade, devido processo legal e ampla defesa. No que diz respeito ao primeiro, o ordenamento jurídico brasileiro fundamenta-se na publicidade dos atos estatais, mecanismo que serve ao controle sobre a racionalidade das decisões (Maia, 2025; Paulo, 2023). Esse princípio é responsável por assegurar a transparência e a motivação dos atos da administração pública e das instâncias decisórias, de modo que toda decisão deve ser compreensível e passível de revisão. Nesse sentido, a publicidade enquanto vetor de legitimidade exige que os cidadãos possam conhecer e avaliar os fundamentos que orientam as escolhas estatais (Maia, 2025; Paulo, 2023).

Entretanto, a opacidade corrói essa garantia ao substituir o dever de fundamentação por conclusões técnicas infensas ao escrutínio público. De acordo com Maia (2025) e Paulo (2023), quando empregados em processos administrativos ou judiciais sem a devida explicitação de seus critérios de funcionamento, os algoritmos opacos comprometem a efetiva inteligibilidade das decisões. Como consequência, a prestação de contas (*accountability*) é enfraquecida (Bioni; Mendes, 2019), fato que fragiliza a confiança pública nas instituições ao impedir o exercício da fiscalização sobre os atos do poder público.

O devido processo legal, por sua vez, representa o conjunto de etapas formais que balizam as intervenções estatais sobre a esfera jurídica individual (Paulo, 2023), assegurando que a atuação do poder público seja pautada pela racionalidade, pela transparência e pelo contraditório. Essa essência garantista é severamente mitigada pela opacidade algorítmica, que inviabiliza a reconstrução do caminho lógico percorrido pelo algoritmo na tomada de determinada providência (Maia, 2025; Paulo, 2023).

Tal princípio pressupõe que o jurisdicionado disponha de paridade de armas, o que demanda a plena compreensão dos fundamentos da decisão como condição para a efetiva participação no processo decisório. Se o algoritmo funciona como uma “caixa-preta” (Pasquale, 2016), o indivíduo é colocado diante de um desfecho que pode não ser plenamente explicado, o que compromete a previsibilidade e a racionalidade exigidas pela ordem constitucional (Paulo, 2023).

O devido processo legal exige, portanto, um espaço de diálogo entre Estado e cidadão, no qual a decisão não é meramente imposta, mas construída em conformidade com regras previamente conhecidas e verificáveis. A opacidade algorítmica fragmenta esse ambiente ao transformar o processo em um mecanismo unilateral, exacerbado por profundas

assimetrias informacionais que anulam a aptidão do sujeito de influenciar o curso do provimento jurisdicional (Maia, 2025; Paulo, 2023). Consequentemente, a ausência de transparência desnatura o caráter “devido” do rito, reduzindo-o a uma sucessão de atos cuja legitimidade escapa ao escrutínio público e jurídico.

De igual modo, a defesa só se realiza plenamente quando há clareza sobre os fundamentos em debate; do contrário, a eficácia do exercício defensivo é esvaziada, tornando-se incapaz de produzir efeitos concretos contra uma lógica técnica inacessível (Greco, 2020). Dessa maneira, a ampla defesa, que pressupõe simetria mínima entre acusação e defesa, perde sua função quando a informação está concentrada em um sistema que não se deixa escrutinar²⁶ (Maia, 2025; Paulo, 2023).

Sob o prisma criminal, a opacidade algorítmica tende a interferir na liberdade de locomoção (Nunes *et al.*, 2025; Silva, 2024). Essa interferência manifesta-se por meio de um efeito inibitório (*chilling effect*),²⁷ segundo o qual o cidadão, por desconhecer os parâmetros que orientam os alertas policiais, vê-se compelido a alterar seus comportamentos e trajetos para evitar abordagens indevidas ou detenções errôneas, decorrentes de falhas algorítmicas que ele não pode prever ou contestar em tempo real (Nunes *et al.*, 2025; Silva, 2024). Assim, quando os critérios de identificação e as margens de erro de determinado sistema de monitoramento

²⁶ Como afirmam Nunes e Marques (2018, p. 429), em sua análise do uso de inteligência artificial na seara do direito processual civil: “Há, contudo, um agravante: as decisões tomadas por humano são impugnáveis, pois é possível delimitar os fatores que ensejaram determinada resposta e o próprio decisor deve ofertar o iter que o induziu a tal resposta [...]. Por outro lado, os algoritmos utilizados nas ferramentas de inteligência artificial são obscuros para a maior parte da população – algumas vezes até para seus programadores – o que os torna, de certa forma, inatacáveis. Em função disso, a atribuição de função decisória aos sistemas de inteligência artificial torna-se especialmente problemática no âmbito do Direito”.

²⁷ O “efeito inibidor” ou “efeito dissuasório” é uma categoria tradicionalmente utilizada na jurisprudência norte-americana para designar a inibição do exercício de direitos decorrente da regulação estatal sobre a governança de conteúdo no ambiente digital (Santini *et al.*, 2025). Embora originalmente aplicado ao ciberespaço, o conceito permite compreender que, também no espaço físico, a autocensura é uma resposta psicológica à assimetria de informação gerada pela vigilância opaca.

biométrico permanecem ocultos, instaura-se um estado de suspeição generalizada.²⁸²⁹³⁰

Rodotà (2008) argumenta que essa falta de transparência também interfere na

²⁸ Nessa linha de raciocínio, ver *Habeas Corpus* (HC) 1.059.475/SP (2025/0487202-0). Malgrado o caso não verse especificamente sobre o reconhecimento facial, a decisão proferida pela Quinta Turma do Superior Tribunal de Justiça (STJ) oferece importante fundamento para a reflexão. No acórdão (Brasil, 2026), discutiu-se a admissibilidade de um relatório técnico produzido por investigador de polícia com o auxílio de ferramentas de inteligência artificial generativa (Gemini e Perplexity), utilizado para sustentar conclusão diversa daquela apresentada pela perícia oficial. O STJ entendeu que o documento não possuía confiabilidade epistêmica mínima para ser utilizado como prova no processo penal, sobretudo porque as ferramentas empregadas não eram adequadas à análise técnica pretendida e porque o resultado produzido não se apoiava em fundamentação científico-metodológica idônea. A Corte também destacou o risco de alucinação inerente à IA generativa e a fragilidade de se atribuir prevalência a um juízo probabilístico em detrimento de perícia oficial realizada por órgão técnico competente. Do julgado, é possível extrair que a tecnologia somente pode adquirir relevância probatória quando sua utilização se submete a critérios mínimos de racionalidade, confiabilidade e controle, visto que a prova penal demanda a possibilidade de reconstrução do percurso que conduziu à conclusão apresentada ao Estado-juiz. É nesse sentido que se afirma que a ocultação dos critérios de identificação e das margens de erro instaura, no âmbito do reconhecimento facial, um estado de suspeição generalizada: a suspeita é difusa porque qualquer pessoa submetida ao campo de visibilidade do sistema pode ser alvo de uma vigilância indiscriminada, mesmo sem compreender ou consentir com os parâmetros empregados pelo algoritmo.

²⁹ A advertência formulada pelo STJ, contudo, não parece encontrar correspondência uniforme na jurisprudência local. Em sentido diverso, o Tribunal de Justiça do Estado do Ceará (TJCE) tem chancelado o emprego de sistemas de inteligência artificial voltados à comparação facial como instrumentos idôneos para a confirmação de identidade no curso de investigações criminais. No julgamento do *Habeas Corpus* nº 0623986-18.2025.8.06.0000, a Primeira Câmara Criminal consignou a validade e a suficiência da identificação de um investigado por intermédio de um *software* de biometria facial. O procedimento consistiu no cruzamento eletrônico entre um registro fotográfico obtido em arquivos atribuídos a organizações criminosas e as imagens arquivadas em bancos de dados oficiais do registro civil, resultando na suposta compatibilidade entre as imagens analisadas (Ceará, 2025c). Em linha semelhante, no âmbito do *Habeas Corpus* nº 0625260-17.2025.8.06.0000, a Terceira Câmara Criminal validou a flexibilização das formalidades do reconhecimento pessoal, assentando que, no caso, o cotejo automatizado supriria as exigências prescritas na legislação processual penal. O Colegiado acolheu como fundamento a identificação realizada por meio de sistema de inteligência artificial que correlacionou uma imagem obtida em serviço de armazenamento digital remoto com os arquivos constantes no banco de dados da Polícia Civil (Ceará, 2025d). A coexistência de interpretações tão díspares evidencia que a incorporação de sistemas automatizados ao rito da persecução penal demanda uma estrutura compatível com a gravidade dos efeitos produzidos pela identificação biométrica. Argumenta-se, então, que a legitimidade dos provimentos jurisdicionais baseados em dados pressupõe a integração da resposta algorítmica a um conjunto probatório amplo, diversificado e corroborado por outros meios autônomos de convicção. Assim, urge a construção de um modelo de governança tecnológica em que as ferramentas computacionais sejam tratadas não como evidências autossuficientes, mas como elementos informativos, cuja validade jurídica deve permanecer condicionada à possibilidade de supervisão humana e de controle técnico dos resultados.

³⁰ Em um processo judicial, a opacidade relativa aos parâmetros lógicos e aos critérios de decisão algorítmica pode interferir diretamente na cadeia de custódia (Costa; Abreu, 2024). Conforme preleciona Badaró (2023; 2024), a cadeia de custódia – entendida como o conjunto de procedimentos destinados a assegurar a integridade, autenticidade e confiabilidade dos elementos probatórios – exige que cada etapa de sua formação seja verificável e passível de contestação. Qualquer ruptura nesse encadeamento compromete a higidez da prova e, por consequência, a legitimidade do provimento jurisdicional que dela se vale (Badaró, 2023; 2024). Nesse contexto, a aplicação de sistemas algorítmicos – notadamente aqueles baseados em inteligência artificial e aprendizado de máquina – introduz no iter processual uma dimensão de incerteza. Sob essa perspectiva, Costa e Abreu (2024, p. 15) sustentam que a interpretabilidade dos modelos de IA é um desafio à seara forense. Afinal, argumentam os autores, quando os parâmetros de funcionamento, as métricas de acurácia e as margens de erro são inacessíveis às partes e ao magistrado, cria-se uma “caixa-preta” probatória. Essa opacidade obstaculiza o exercício do contraditório pleno, uma vez que não se pode impugnar o que não se pode compreender. Em última análise, a ausência de transparência algorítmica pode equivaler a uma quebra da cadeia de custódia, na medida em que inviabiliza a rastreabilidade e a auditabilidade do percurso da prova.

autonomia privada e na autodeterminação informativa,³¹ direitos que pressupõem uma vontade livre e informada, a fim de garantir ao indivíduo o controle sobre seus dados e sobre a projeção de sua identidade social. A prática do perfilamento (Eubanks, 2018; Noble, 2018; O’Neil, 2017; Zuboff, 2018) viola essas prerrogativas ao atribuir riscos, preferências e comportamentos ao sujeito de forma arbitrária (Rodotà, 2008). O resultado dessa tensão é a criação de um *déficit* democrático que alcança o núcleo da legitimidade constitucional e deturpa a função pedagógica e fiscalizatória do Direito.

O desafio contemporâneo consiste, pois, em equilibrar inovação tecnológica e garantias fundamentais. A discussão sobre responsabilidade, desenvolvida no tópico seguinte, depende da possibilidade de identificar não apenas os agentes humanos envolvidos na concepção, implementação e supervisão dos sistemas, mas também os critérios e os dados que orientam as escolhas feitas pelos computadores.

3.6 Agência e responsabilidade sobre a decisão automatizada: a centralidade do elemento humano

A integração de sistemas de inteligência artificial no cerne das instituições jurídicas e de segurança pública reconfigura os paradigmas de agência e imputabilidade. Esta seção dedica-se à análise sobre a responsabilidade pelas decisões automatizadas, sobretudo considerando a transposição de vieses para as arquiteturas computacionais (Frazão, 2023). Parte-se, então, da premissa de que a aplicação do Direito e o exercício da força estatal possuem natureza ética e dependem da presença de um sujeito capaz de reconhecer e ser reconhecido dentro de uma comunidade moral (Greco, 2020; Oliveira, 2020; Viana, 2021).

Como visto em tópicos anteriores, na alçada técnica, os sistemas de inteligência artificial realizam o processamento estatístico de dados a partir de parâmetros previamente definidos (Oliveira, 2020; Domingos, 2017a; Russell; Norvig, 2010). Embora apresentem capacidade adaptativa por meio do aprendizado de máquina e do aprendizado profundo (Corrêa,

³¹ Rodotà (2008) explica que, na era digital, o indivíduo possui dois corpos: o corpo físico e o corpo eletrônico, isto é, uma projeção da identidade do sujeito no mundo digital. Este último é composto por um rastro de dados, e perder o controle sobre esses dados significa perder parte da própria liberdade e dignidade. O autor defende que o conceito clássico de privacidade (o “direito de ser deixado só”) era insuficiente em uma sociedade de vigilância. No mundo hiperconectado, a privacidade deve ser vista como uma ferramenta de participação e controle. Assim, sendo o acúmulo de informações uma forma de poder, que cria um desequilíbrio entre cidadãos, grandes corporações e o Estado, a autodeterminação informativa representaria uma ferramenta de defesa da democracia, ao garantir aos cidadãos o poder jurídico de acompanhamento, intervenção e decisão sobre o destino de suas informações pessoais.

2021; Kaufman, 2020; Hoffmann-Riem, 2020), sua estrutura permanece fundada em escolhas humanas (Greco, 2020) relativas à finalidade do sistema, à seleção de variáveis, à composição das bases de treinamento e à definição de critérios de validação (Domingos, 2017b; Crestane; Leal, 2024; Russell; Norvig, 2010; Kleinberg *et al.*, 2018).

A presença humana em determinadas etapas não implica, porém, desenvolvimento de efetiva cognição (Oliveira, 2020; Searle, 2006). Isso significa que os processos de funcionamento dos algoritmos, regidos pela causalidade estatística, se distinguem qualitativamente da consciência humana. Esta, compreendida como a base da responsabilidade moral, permite que o indivíduo perceba o significado de suas ações e o impacto destas sobre terceiros, diferentemente do que ocorre com ferramentas computacionais (Greco, 2020; Oliveira, 2020; Searle, 2006; Viana, 2021).

A intencionalidade humana define-se pela aptidão da mente em conferir significado e propósito a objetos e estados de coisas (Oliveira, 2020; Searle, 2006; Quaresma, 2020). Um estado mental intencional possui conteúdo e alvo, processados a partir de uma vivência subjetiva e orientada – seja a algo real, imaginário ou abstrato. No que tange aos sistemas artificiais, o que se observa é uma simulação de intencionalidade: a máquina processa símbolos de acordo com regras sintáticas, sem apreender o valor intrínseco dessas informações (Searle, 2006). Assim, a autonomia técnica da inteligência artificial limita-se ao ajuste de parâmetros internos sem intervenção humana direta, permanecendo, contudo, desprovida de autonomia moral (Oliveira, 2020).

Nessa conjuntura, a tentativa de personificar a tecnologia deslocaria o foco do problema sem solucioná-lo, visto que o ato de decidir requer discernimento, subjetividade e agência voluntária (Normando, 2012; Russell; Norvig, 2010). Falta ao código a estrutura biopsicossocial que possibilita aos humanos perceber nuances históricas, culturais e políticas; seu processo decisório é condicionado por sua programação e pelos dados que o alimentam (Oliveira, 2020; Searle, 2006). Enquanto o ser humano possui estados psíquicos dirigidos a determinados fins, podendo questionar o seu objetivo e alterá-lo com base em reflexões éticas, as ações da inteligência artificial derivam da otimização de funções de custo, e não de uma escolha livre entre valores conflitantes (Oliveira, 2020; Searle, 2006; Viana, 2021). Trata-se de uma racionalidade estritamente instrumental, que não se confunde com a racionalidade prática da ética (Russell; Norvig, 2010).

Greco (2020) elucida que a responsabilidade no ordenamento jurídico pressupõe um sujeito dotado de compreensão e autodeterminação,³² atributos que transcendem o mero cálculo matemático. Nesse sentido, atribuir responsabilidade a um algoritmo equivaleria a reconhecer a possibilidade de uma máquina ser detentora de personalidade jurídica, motivo pelo qual modelos computacionais situam-se fora do escopo tradicional das normas de responsabilização.

Dessa forma, a imposição de multas ou a desativação do sistema não cumprem a função retributiva ou pedagógica da sanção jurídica, pois o destinatário da punição é indiferente ao seu significado. Sob essa perspectiva, mais eficaz seria a reconstrução da cadeia decisória, abrangendo desde desenvolvedores até gestores públicos e autoridades que optam por incorporar essas ferramentas ao processo administrativo ou judicial (Oliveira, 2020; Viana, 2021; Martins *et al.*, 2024; Nunes; Marques, 2018; Nunes *et al.*, 2025).

No âmbito da segurança pública, a ausência de consciência moral em ferramentas de reconhecimento facial impede que a tecnologia avalie a justiça ou a validade ética dos dados processados (Duarte; Nunes; Lima, 2023; Martins *et al.*, 2024; Nunes *et al.*, 2025). Ao passo que um agente humano pode questionar a procedência de uma informação ou identificar vieses discriminatórios, o *software* tende a espelhar e amplificar essas assimetrias. Por essa razão, a supervisão humana é uma medida de segurança indispensável à utilização de tais mecanismos (Oliveira, 2020; Corrêa, 2021; Nunes *et al.*, 2025).

A omissão na correção de vieses, ou mesmo a opção consciente por sistemas com taxas de erro conhecidas, constitui uma conduta voluntária. Nessa perspectiva, embora o algoritmo permaneça como o meio de manifestação do dano, a agência moral recai sobre o indivíduo que autoriza sua aplicação em determinado contexto social. Assim, falhas algorítmicas, como as verificadas em tecnologias de reconhecimento facial, devem ser interpretadas como violações diretas do dever de diligência (Duarte; Nunes; Lima, 2023; Martins *et al.*, 2024; Nunes *et al.*, 2025).

Sob essa ótica, Brayne (2021) explica que a associação entre setor público e empresas privadas de tecnologia visa à criação de um “vácuo de responsabilidade”. A autora

³² Não obstante, a posição adotada neste trabalho sustenta que a responsabilização jurídica de agentes humanos, instituições públicas e empresas privadas também deve ser estruturada a partir de encargos objetivos de diligência, governança, prevenção de danos e prestação de contas, sem que isso implique qualquer oposição ao aspecto subjetivo.

sustenta que a administração estatal frequentemente se dissocia da responsabilidade por falhas em sistemas adquiridos de terceiros, transferindo sua discricionariedade decisória ao externalizar o desenvolvimento de tais ferramentas. Esse processo permite ao Estado usufruir de um incremento na eficácia e na otimização da vigilância, ao passo que o preserva do ônus político e jurídico da transparência.

A incorporação dessas tecnologias, amiúde dissociada de marcos regulatórios precisos, faculta às entidades privadas a prerrogativa de delimitar os critérios de êxito ou erro no campo da segurança pública. O Estado assume uma posição de consumidor passivo desses parâmetros, o que, segundo Brayne (2021), resulta na dispensa da fundamentação sociopolítica de suas opções administrativas. A autora argumenta que esse recurso de blindagem algorítmica fragiliza os alicerces do Estado de Direito, visto que a transparência e o devido processo legal são preteridos em favor de uma eficiência operacional cujas métricas de controle são estabelecidas e geridas por entes privados, subtraindo-as do escrutínio democrático convencional.

Eubanks (2018) acrescenta que a delegação de prerrogativas decisórias a algoritmos impacta severamente a integridade das políticas públicas. De acordo com a teórica, a “automação das desigualdades” desloca o eixo da gestão estatal: em vez de enfrentar as causas estruturais da desigualdade, como a precarização do trabalho e a concentração de renda, o Estado limita-se a administrar os sintomas dessas disparidades. Nesse percurso, o emprego de sistemas automatizados com a finalidade de gerenciar serviços públicos tende a excluir as camadas mais vulneráveis da sociedade, privando-as do acesso a direitos básicos, como saúde, moradia e assistência social.

A legitimidade das tecnologias, notadamente as de reconhecimento facial, depende, portanto, da possibilidade de controle e fiscalização humana, da definição clara de deveres institucionais e da observância das garantias fundamentais. O capítulo subsequente examinará como essas questões se materializam no contexto específico do estado do Ceará, analisando a implementação do reconhecimento facial, os riscos associados à sua utilização e as possíveis implicações jurídicas resultantes das problemáticas aqui discutidas.

4 SELETIVIDADE PENAL E OS LIMITES DA APLICAÇÃO DE TECNOLOGIAS BIOMÉTRICAS NA SEGURANÇA PÚBLICA CEARENSE

O presente capítulo propõe uma análise da ascensão das tecnologias de reconhecimento facial como eixos centrais das novas estratégias de segurança pública, problematizando sua integração ao contexto social e institucional do Ceará. Após a construção teórica acerca da sociedade de controle, da racionalidade algorítmica, dos vieses e da opacidade decisória, a investigação desloca-se para o modo como esses elementos se articulam em uma infraestrutura concreta de vigilância.

A primeira seção apresenta uma exposição sobre o funcionamento das tecnologias de reconhecimento facial, descrevendo seus principais estágios de processamento, desde a detecção e extração de características biométricas até os equipamentos de verificação e identificação. Busca-se, com isso, evidenciar como variáveis ambientais e escolhas de *design* impactam diretamente a confiabilidade dos resultados. Ao situar o reconhecimento facial no interior de uma racionalidade sociotécnica (Feenberg, 2013), o tópico também estabelece as bases para compreender tais tecnologias como expressões contemporâneas de vigilância orientada por dados.

A investigação prossegue com a territorialização desse debate no estado do Ceará, mapeando a trajetória do videomonitoramento desde a sua implementação para megaeventos esportivos até a consolidação de uma infraestrutura securitária impulsionada pelo programa *Cientista-Chefe* (Matos *et al.*, 2020; Chaves, 2025; Santaella, 2025). Analisa-se a criação de plataformas tecnológicas que centralizam fluxos de dados governamentais para orientar a repressão à criminalidade. Ao mesmo tempo, evidencia-se a ausência de parâmetros normativos uniformes e a limitação de informações disponíveis sobre o funcionamento efetivo dessas ferramentas, salientando o padrão de opacidade institucional da segurança pública cearense. Ademais, problematiza-se o papel do discurso na legitimação dessas tecnologias, demonstrando como a associação entre segurança e inovação tecnológica contribui para a consolidação de um paradigma de controle orientado pelo solucionismo tecnológico (Morozov, 2013).

A crítica é desenvolvida a partir da teoria do etiquetamento (Becker, 2008; Goffman, 1981; Lemert, 1967) e do conceito de sujeição criminal (Misse, 1999; 2006; 2008; 2009; 2010). Nesse sentido, o texto examina a construção social da criminalidade e a produção de identidades desviantes, articulando essas dinâmicas ao contexto brasileiro e, de modo

específico, à realidade cearense. Dados empíricos a respeito do encarceramento e da letalidade policial no Ceará são utilizados para evidenciar a sobrerrepresentação da população negra nas estatísticas criminais. Nesse cenário, demonstra-se como a incorporação de sistemas algorítmicos tende a reproduzir e intensificar padrões preexistentes de discriminação, sobretudo diante da utilização de acervos de dados enviesados. O tópico é ilustrado por casos emblemáticos que revelam falhas técnicas e erros de identificação, permitindo observar concretamente os riscos associados ao uso dessas tecnologias.

Por fim, o capítulo debruça-se sobre os desafios impostos pela Lei Geral de Proteção de Dados, destacando o vácuo jurídico criado pela exclusão das atividades de segurança pública de seu escopo de aplicação principal, o que expande a margem de atuação estatal sem a correspondente institucionalização de mecanismos de controle e responsabilização. A discussão inclui, ainda, exemplos de propostas legislativas voltadas à regulamentação desse campo e de suas fragilidades, destacando a indispensabilidade de construção de um arcabouço normativo capaz de assegurar transparência, auditabilidade e contestabilidade no emprego de tecnologias de vigilância.

A partir desse encadeamento, o capítulo permite compreender os riscos sociotécnicos associados aos sistemas de reconhecimento facial e propõe uma reflexão crítica sobre a necessidade de salvaguardas que assegurem o respeito às garantias fundamentais do Estado Democrático de Direito.

4.1 Considerações gerais sobre o funcionamento das tecnologias de reconhecimento facial

Malgrado a relação entre o *big data* e a estruturação de uma sociedade de controle não seja recente (Frazão, 2019, p. 27), o monitoramento ostensivo alcançou novos níveis de sofisticação a partir do desenvolvimento recente de modelos algorítmicos capazes de processar grandes volumes de informações em tempo real (Cath *et al.*, 2017). Esse avanço tecnológico viabilizou a automação de processos burocráticos e administrativos, anteriormente condicionados ao tempo e à discricionariedade humana (Bioni, 2020), inserindo-se em um movimento mais abrangente de busca por eficiência na gestão pública (Bioni, 2020; Martins *et al.*, 2024).

Nesse contexto, Han (2018, p. 78) identifica a emergência de uma forma ampliada de controle, caracterizada pela capacidade de oferecer “uma visão em 360° dos seus internos”, nos moldes da dimensão difusa e permanente descrita por Deleuze (1992). O filósofo denomina

essa modalidade de vigilância de “panóptico digital”, cuja eficácia decorre de sua estrutura aperspectivista, capaz de suprimir limitações inerentes à óptica analógica. Conforme expõe o autor, a “óptica digital possibilita a vigilância a partir de qualquer ângulo. Assim, elimina pontos cegos” (Han, 2018, p. 78).

A incorporação de algoritmos de inteligência artificial a esse cenário resulta de uma racionalidade sociotécnica³³ (Feenberg, 2013; 2017), que conferiu maior acurácia às intervenções estatais (Feenberg, 2013; Dignam, 2020) mediante a ampliação da capacidade de delegação de funções decisórias a estruturas computacionais (Biondi, 2018; Martins *et al.*, 2024). A partir desses sistemas, verificou-se uma reorganização das práticas policiais em termos de planejamento e execução: por meio dessa arquitetura, as forças de segurança puderam processar grandes volumes de registros criminais, dados geoespaciais e imagens de monitoramento em tempo real (Bruno, 2013; Duarte; Nunes; Lima, 2023; Martins *et al.*, 2024).

Entre as aplicações mais expressivas dessa transformação situa-se o reconhecimento facial. Essa tecnologia consiste em um processo automatizado de análise biométrica (Bowen, 2022; Hamann; Smith, 2019; Madiega; Mildebrath, 2021; Pereira, 2022; Souza; Zanatta, 2021) que extrai padrões geométricos e vetoriais da face humana, denominados pontos nodais, com a finalidade de determinar a identidade de um indivíduo. A verificação, realizada em tempo real ou por meio de registros previamente armazenados, é feita a partir da comparação entre o mapa facial e diferentes bases de dados (Bowen, 2022; Hamann; Smith, 2019; Madiega; Mildebrath, 2021; Pereira, 2022; Souza; Zanatta, 2021).

O funcionamento desses sistemas envolve múltiplos estágios de processamento. Inicialmente, ocorre a detecção facial, etapa em que redes neurais especializadas identificam a presença de um rosto humano em um determinado enquadramento digital (Souza; Zanatta, 2021). Essa fase apresenta elevada sensibilidade a variáveis nas condições ambientais³⁴ (Zeng;

³³ Em sua teoria da dupla instrumentalização, Feenberg (2013) propõe uma abordagem que reconhece as tecnologias como resultado da interação entre seu aspecto funcional e sua dimensão social. Isso significa que, embora funcionem por meio da lógica matemática, as tecnologias são permeadas pelas subjetividades humanas. A partir disso, Feenberg desenvolve o conceito de “racionalidade sociotécnica”, que articula o componente singular – isto é, o uso instrumental e técnico de uma tecnologia – com sua face social, marcada pelos valores, interesses e significados que se cristalizam na materialidade do objeto técnico. De acordo com essa teoria, toda tecnologia carrega em si uma dupla inscrição: de um lado, responde a exigências práticas de eficiência, desempenho e solução de problemas; de outro, incorpora escolhas sociais, culturais e políticas que orientam sua concepção e aplicação. Em suma, a teoria de Feenberg desloca o olhar da tecnologia como mera ferramenta para entendê-la como um campo de disputa simbólica e material, no qual diferentes grupos imprimem suas concepções de mundo.

³⁴ Como discutido no capítulo anterior, sistemas de captura biométrica são frequentemente otimizados para tons de pele mais claros (Buolamwini; Gebre, 2018; Benjamin, 2019; Solarova *et al.*, 2023). Nesse contexto, Reis (2025) explica que, em ambientes com iluminação subótima ou com presença de sombras, a pele retinta absorve

Qiu; Shi, 2021; Reis, 2025), como iluminação, ângulo de captura e resolução da imagem, fatores que influenciam diretamente a qualidade dos dados extraídos, a estabilidade do reconhecimento (Souza; Zanatta, 2021) e a confiabilidade dos resultados, podendo haver maior ou menor ocorrência de falsos positivos (Buolamwini; Gebru, 2018; Benjamin, 2019; Reis, 2025).

Na sequência, realiza-se o alinhamento e a extração de características morfológicas, momento em que o *software* mapeia marcos faciais específicos, conhecidos como *landmarks* (Bowen, 2022; Madiega; Mildebrath, 2021; Souza; Zanatta, 2021). Esses pontos incluem, entre outros, a distância entre os centros das pupilas, a largura do nariz, o contorno das maçãs do rosto, a estrutura da mandíbula e a profundidade das órbitas oculares. A partir desses dados, é construído um vetor numérico representativo da face analisada, que será a base para a etapa de comparação (Souza; Zanatta, 2021).

Conforme descrevem Souza e Zanatta (2021), a etapa final consiste no reconhecimento propriamente dito, isto é, na classificação de imagens em contextos variados, que pode ocorrer de dois modos distintos: verificação e identificação. Na primeira, o sistema compara a imagem capturada com uma única referência previamente cadastrada, com o objetivo de confirmar a identidade alegada por determinado usuário, prática comum no desbloqueio de dispositivos móveis ou no controle de acesso em aeroportos. Na identificação, por sua vez, a comparação ocorre em relação a um conjunto amplo de imagens armazenadas em bases de dados governamentais ou privadas, visando determinar a identidade de sujeitos desconhecidos.

No âmbito da segurança pública, esses sistemas articulam-se a modelos preditivos que utilizam dados históricos³⁵ de ocorrências criminais, padrões geográficos e comportamentais para identificar áreas com maior probabilidade de incidência criminal (Weisburd; Telep, 2014). Essa metodologia contribui para a alocação preventiva de recursos

maior quantidade de luz, o que pode resultar na perda de definição de pontos nodais. De modo semelhante, quando a resolução da imagem é baixa ou o ângulo de captura é oblíquo, o ruído dificulta a diferenciação entre os traços faciais e o cenário, ou entre sombras e características anatômicas. Esse conjunto de limitações pode culminar em falsos positivos, situações em que o sistema algorítmico falha ao distinguir indivíduos diferentes com tons de pele semelhantes, agrupando-os em categorias genéricas por não conseguir processar as nuances da face. À vista disso, o autor conclui que, em situações de vigilância de massa, a incapacidade de capturar, processar e reconhecer perfeitamente uma imagem, somada aos vieses presentes nos conjuntos de dados de treinamento, afeta desproporcionalmente pessoas negras.

³⁵ Dados históricos compreendem o rastro digital sobre comportamentos, decisões e medições acumulado ao longo do tempo, sendo empregados no treinamento de modelos de inteligência artificial e *machine learning* (Floridi, 2014). O'Neil (2017) explica que, quando registros enviesados são utilizados em novas decisões, cria-se um *feedback loop*: resultados tendenciosos voltam a ser usados como dados de entrada para decisões futuras, que serão igualmente tendenciosas, reforçando o erro inicial.

policiais em “pontos quentes” (*hotspots*)³⁶ (Weisburd; Telep, 2014), sendo frequentemente associada à ampliação da capacidade estatal de gestão de dados e planejamento estratégico (Martins *et al.*, 2024; Kremer; Nunes; Lima, 2023).

Todavia, conforme discutido anteriormente, a objetividade atribuída aos algoritmos biométricos deriva de processos de simplificação que impõem limites à representação da experiência humana (Pasquale, 2016; Morozov, 2013) – dinâmicas históricas, políticas, econômicas e culturais são, por vezes, invisíveis à tecnologia. Por esse motivo, a implementação de sistemas invasivos no âmbito da segurança pública deve considerar as escolhas éticas feitas desde o seu *design* (Morozov, 2013; O’Neil, 2017; Noble, 2018), a fim de evitar o solucionismo tecnológico³⁷ (Morozov, 2013; Marx, 2024), cuja lógica, no contexto do estado do Ceará, desafia o controle democrático ao restringir a possibilidade de escrutínio público e de contestação por parte dos indivíduos afetados (Duarte; Nunes; Lima, 2023; Lins, 2020; Martins *et al.*, 2024).

4.2 Infraestrutura de vigilância e integração tecnológica na segurança pública do estado do Ceará

No Brasil, a aplicação do reconhecimento facial como parte de uma infraestrutura de vigilância orientada por dados, conforme delineado no tópico anterior, encontra seus marcos iniciais na preparação para megaeventos, como a Copa do Mundo de 2014 e os Jogos Olímpicos de 2016 (Duarte; Nunes; Lima, 2023; Martins *et al.*, 2024; Cardoso, 2018, p. 93). Foi, porém, em 2019 que a adoção de tecnologias biométricas ganhou maior destaque (Nunes *et al.*, 2025), sobretudo com a Portaria nº 793/2019 (Brasil, 2019). A partir dela, foi autorizada a utilização de recursos do Fundo Nacional de Segurança Pública para a aquisição de sistemas de videomonitoramento dotados de reconhecimento facial, inteligência artificial e tecnologias correlatas (Brasil, 2019; Silva; Xavier, 2025).

A ausência de uma regulação federal unificada, contudo, conduz a um processo de expansão heterogêneo, sem a observância de parâmetros éticos e técnicos uniformes (Duarte;

³⁶ Na segurança pública, *hotspots*, ou pontos críticos, são áreas geográficas de pequena escala que registram níveis de criminalidade significativamente superiores à média da jurisdição em que se inserem. O conceito sugere que o crime não se distribui de maneira uniforme; ao contrário, se concentra em pequenas localidades onde a convergência de fatores ambientais e sociais facilita a atividade ilícita, o que justificaria o direcionamento de recursos e a intensificação do policiamento nessas regiões (Weisburd; Telep, 2014).

³⁷ O solucionismo tecnológico, ou tecnosolucionismo, remete à crença de que todos os dilemas humanos são passíveis de resolução por meio da aplicação de soluções tecnológicas (Marx, 2024, p. 85).

Nunes; Lima, 2023; Martins *et al.*, 2024). Nesse sentido, um mapeamento realizado pelo projeto *O Panóptico*, monitor de tecnologias de segurança vinculado ao CESeC, indica a existência de 535 iniciativas ativas no país, o que submete aproximadamente 97 milhões de cidadãos a mecanismos de monitoramento biométrico, sem a correspondente padronização legal.³⁸

No Ceará, a trajetória do videomonitoramento iniciou-se entre os anos de 2013 e 2014, durante a preparação para a Copa das Confederações e a Copa do Mundo (Martins *et al.*, 2024; Silva; Xavier, 2025). Nesse período, o governo estadual inaugurou o Centro Integrado de Comando e Controle (CICC) do Nordeste, que permitiu a instalação de centenas de câmeras conectadas a uma central de monitoramento em Fortaleza (Martins *et al.*, 2024, p. 5; Silva; Xavier, 2025). A partir de então, o estado firmou diversas parcerias estratégicas com instituições acadêmicas, notadamente a Universidade Federal do Ceará (UFC) e o Laboratório de Processamento de Imagem, Sinais e Computação (Lapisco), vinculado ao Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE) (Holanda, 2024; Silva, 2025a). Essa cooperação viabilizou o desenvolvimento de sistemas de análise de dados e videomonitoramento inteligente customizados às demandas locais (Holanda, 2024; Silva, 2025a).

A modernização da infraestrutura securitária cearense acelerou-se com a instituição do programa *Cientista-Chefe*, regulamentado pela Lei Estadual nº 17.378/2021 (Ceará, 2021a; Matos *et al.*, 2020; Chaves, 2025; Santaella, 2025). A iniciativa tem o intuito de promover o desenvolvimento de *softwares* e plataformas de inteligência artificial adaptados às necessidades da Secretaria da Segurança Pública e Defesa Social (SSPDS-CE) (Matos *et al.*, 2020; Chaves, 2025; Santaella, 2025). Entre os principais produtos dessa colaboração, destaca-se a *Plataforma Multibiométrica e Monitoramento Inteligente* (Ceará, [s.d.]a), que visa integrar o reconhecimento facial aos bancos de dados civis e criminais existentes no estado.

Apesar da relevância atribuída ao projeto, no momento de escrita desta monografia, não foram encontradas informações detalhadas sobre os critérios de operação da plataforma, em uma manifestação da opacidade que permeia as instituições cearenses e limita o escrutínio público. Nessa perspectiva, ressalta-se, uma vez mais, que a indisponibilidade de dados impede a avaliação independente da acurácia, dos vieses e dos impactos dessas tecnologias, fato que inviabiliza a contestação qualificada dos resultados e, por conseguinte, produz uma assimetria

³⁸ Os dados referem-se à atualização de 28 de abril de 2026, conforme informações disponibilizadas no site oficial do projeto *O Panóptico*. Disponível em: <https://www.opanoptico.com.br/#mapa>. Acesso em: 12 maio 2026.

significativa entre o Estado e os seus cidadãos.

Ainda no âmbito do programa *Cientista-Chefe*, foram desenvolvidos outros *softwares* analíticos voltados à gestão operacional da segurança. O Sistema Policial Indicativo de Abordagem (SPIA), por exemplo, é fruto de uma parceria entre a SSPDS-CE, a Polícia Rodoviária Federal (PRF) e a UFC (Lins, 2020, p. 79-82; Ceará, 2023). A ferramenta utiliza inteligência artificial para processar imagens de videomonitoramento e sensores dispostos pela cidade, a fim de identificar veículos roubados, furtados ou clonados e rastrear trajetos em tempo real (Ceará, 2019). Adicionalmente, o Sistema Tecnológico para Acompanhamento de Unidades de Segurança (STATUS) realiza análises estatísticas e geoespaciais para identificar zonas de maior incidência criminal, orientando a distribuição de recursos e a definição de estratégias de repressão à criminalidade (Ceará, [s.d.]b; 2021b).

O núcleo de processamento dessa estrutura é o painel analítico *Odin*, que centraliza volumosos fluxos de dados provenientes de mais de uma centena de fontes governamentais e de instituições parceiras (Ceará, [s.d.]b; 2019). Essas informações alimentam o sistema de *big data Cerebrum* (Silva, 2025a), responsável por análises preditivas e cruzamento de registros biográficos e criminais. A integração entre ambos os sistemas possibilita a construção de redes relacionais entre indivíduos, antecedentes criminais e dados civis, ampliando a capacidade investigativa de delitos complexos (Ceará, [s.d.]b; 2019).

O reconhecimento facial constitui parte essencial desse ecossistema, operando tanto em estruturas fixas (Castro, 2025), por intermédio das câmeras do Núcleo de Videomonitoramento (Nuvid), quanto em dispositivos móveis, utilizados em abordagens policiais (Ceará, 2020a; 2020b; 2020c; 2020d; 2025a). Nesse contexto, destaca-se o Portal de Comando Avançado (PCA), desenvolvido em parceria com a UFC. Trata-se de um aplicativo para *smartphones*, de uso exclusivo dos servidores da segurança pública, que exemplifica essa dinâmica de integração tecnológica. A partir da captura de imagens faciais, a ferramenta oferece funcionalidades de consulta biométrica e criminal, permitindo a obtenção imediata de correspondências em bases de dados estaduais (Ceará, [s.d.]b, p. 89-92; 2020a; 2020b; 2020c; 2020d).

Essa infraestrutura de vigilância vem sendo significativamente expandida pelo governo estadual. Em agosto de 2024, o governador Elmano de Freitas (PT) anunciou o programa *Ceará contra o Crime*, que institucionalizou o projeto *Identifica Ceará* (Silva;

Xavier, 2025; Falcão, 2024). Essa política pública prevê a ampliação em larga escala do reconhecimento facial e a integração de sistemas de câmeras privadas à base de dados da SSPDS-CE (Falcão, 2024), ampliando o alcance estatal em áreas ainda não contempladas pelo videomonitoramento público. Conforme declarado pelo governador (Falcão, 2024), o objetivo central do projeto consiste na captura de foragidos da justiça e na localização de pessoas desaparecidas, mediante o uso de uma base de dados que reúne informações de diferentes esferas governamentais.

No plano municipal, a gestão do prefeito Evandro Leitão (PT), em parceria com o governo estadual, inaugurou o Centro Integrado de Videomonitoramento de Fortaleza (CIVFor). A entrega do equipamento, fruto do programa *FORtaleCE*, ocorreu em 7 de abril de 2026, durante as comemorações alusivas aos 300 anos de fundação da capital cearense (Ceará, 2026; Fortaleza, 2026; Freire; Barbosa, 2026). A vinculação cronológica e simbólica entre a efeméride e a ampliação das redes de monitoramento descortina a orientação político-institucional assumida pela governamentalidade local, pautada no adensamento de uma infraestrutura de vigilância indiscriminada. Em vez de assinalar o terceiro centenário da cidade com a expansão de bens comuns, espaços públicos de fruição coletiva ou políticas estruturais de inclusão, a data comemorativa foi instrumentalizada como esteira de legitimação para uma engenharia de controle socioespacial, respaldada por uma retórica palatável de combate à criminalidade.

Essa conjuntura ilustra, ainda, uma reconfiguração da dinâmica citadina em direção a um modelo de monitoramento multissetorial. Segundo a municipalidade, o projeto articula-se com diversas instâncias institucionais, como SSPDS-CE, Guarda Municipal, Defesa Civil, Agência de Fiscalização de Fortaleza (Agefis), Empresa de Transporte Urbano de Fortaleza (Etufor), Autarquia Municipal de Trânsito e Cidadania (AMC), Secretaria Municipal da Educação (SME) e Polícia Militar do Ceará (PMCE), entre outras (Ceará, 2026; Fortaleza, 2026; Freire; Barbosa, 2026). Essa integração denota que a racionalidade tecnossolucionista descrita por Morozov (2013) ultrapassa os aparatos policiais convencionais e se projeta sobre múltiplas camadas da administração pública – alcançando desde a regulação do tráfego e do transporte coletivo até a governança do ambiente escolar.

Conforme mencionado anteriormente, por meio do *chilling effect* (Santini *et al.*, 2025), essa constante sujeição do corpo social a dispositivos de inteligência artificial nos eixos de maior circulação urbana constrange o pleno exercício dos direitos à privacidade, à intimidade

e à proteção de dados pessoais, bem como inibe, no espaço público, as liberdades de reunião, associação e livre manifestação do pensamento. Nesse prisma, o CIVFor, mais do que uma efetiva celebração da cidade de Fortaleza, legou à coletividade um complexo tecnológico que normaliza a vigilância como componente ordinário da vida cotidiana e engendra processos de estigmatização de seus próprios cidadãos.

Sob a coordenação da Secretaria Municipal da Segurança Cidadã (Sesec), o centro dispõe de um sistema inteligente de videomonitoramento, com mais de 7 mil câmeras integradas – das quais 1.160 são compartilhadas com as forças de segurança estaduais. Esses equipamentos contam com tecnologia de visão noturna, visão de 360 graus e recursos de inteligência artificial, estando interligados à Coordenadoria Integrada de Operações de Segurança (Ciops) (Ceará, 2026; Fortaleza, 2026; Freire; Barbosa, 2026).

Segundo o secretário da Segurança Cidadã, a disposição das câmeras considera, entre outros fatores, áreas de grande fluxo populacional e locais de maior risco de violência (Freire; Barbosa, 2026). Sob essa perspectiva, a prefeitura e o governo estadual defendem que o CIVFor contribuirá, por exemplo, para a segurança no entorno de instituições de ensino e unidades de saúde, bem como para a detecção de atividades suspeitas (Ceará, 2026). A ausência de informações detalhadas sobre o funcionamento das tecnologias empregadas no CIVFor, entretanto, reforça o padrão de opacidade institucional visto anteriormente, dificultando a avaliação de seus impactos e limites.

Ainda assim, a comunicação institucional busca legitimar a nova estrutura de vigilância da capital cearense. Durante a inauguração do CIVFor, o governador enfatizou que o equipamento atuará tanto na prevenção quanto na repressão de ocorrências. Além disso, declarou a intenção de ampliar o uso de inteligência artificial nas câmeras de monitoramento urbano. Em suas palavras: “Não tenho nenhuma dúvida de que essa Inteligência Artificial vai dizer se, numa rua, tem alguém com uma arma apontada. [...] Fortaleza estava entre as cidades mais violentas do Brasil; agora, devemos estar entre as menos” (Freire; Barbosa, 2026).

A declaração do governador exemplifica um discurso orientado pelo solucionismo tecnológico (Morozov, 2015), deslocando o debate das causas sociais da violência para soluções técnicas de controle. Assim, em um cenário marcado pela criminalidade (Feltran *et al.*, 2022; Chaves, 2025; Silva, 2025a; Lins, 2020) e pela violência urbana (Paraná; Santaella, 2025, p. 13), inclusive pela violência policial (Barreto; Ferreira, 2023; Patz, 2024; Melo; Serra,

2022; Silva; Xavier, 2025; Paiva, 2019; Oliveira Silva Filho; Mariano, 2020), Lins (2020, p. 74) observa que discursos de combate ao crime, notadamente ao avanço das organizações criminosas³⁹ (Nascimento; Freitas, 2019; Barros *et al.*, 2018; Benício *et al.*, 2018; Paiva, 2018; Comitê..., 2016), possuem papel fundamental na legitimação de situações de exceção na segurança pública cearense. De acordo com a autora:

No Ceará, essa guerra ao crime, sobretudo às facções e aos grupos criminosos nos últimos anos, tem sido usada como elemento fundante de grandes operações policiais. Mais do que isso, acaba por ser a justificativa perfeita para resultados desastrosos. [...] A operação policial, militarizada e com uso de tecnologias, passou a ser a única forma de pensar a resolução dos conflitos (Lins, 2020, p. 74).

Santaella (2025, p. 13) propõe um raciocínio semelhante, destacando que a captura massiva e indiscriminada de dados – prática que se aproxima de uma “vigilância de arrasto” ou *bulk surveillance*⁴⁰ (Murray; Fussey, 2019) – pode intensificar a negação de direitos a parcelas vulneráveis da população cearense. Para o pesquisador:

No campo da segurança pública, os usos são apresentados como forma de mitigar as enormes ondas de violência urbana que atingem a sociedade cearense, particularmente a juventude periférica. Entretanto, ao defender a captura massiva e indiscriminada de dados e consequentemente o método da chamada vigilância de arrasto, os riscos emergem rapidamente: um modelo de segurança pública que confia no solucionismo

³⁹ Em pesquisa desenvolvida no âmbito do Laboratório de Estudos da Violência (LEV), da UFC, Paiva (2019) desnudou o aprofundamento da crise na segurança pública cearense, sobretudo na capital, a partir da substituição das antigas gangues territoriais por coletivos criminais organizados, popularmente conhecidos como “facções”. Como demonstra o pesquisador, essa mudança representa uma nova forma de governança sobre as populações periféricas, alimentada pela omissão e pela violência institucional do Estado, fatores que ofereceram as condições objetivas para o processo de adesão às organizações, alterando radicalmente as “maneiras de fazer o crime” na cidade. De acordo com o autor, “a colaboração e a omissão dos Governos Federal e Estadual permitiram que jovens fossem integrados em uma sociedade de classes, injusta e desigual, por meio da violência e da morte sistemática de seus parentes e amigos” (Paiva, 2019, p. 181). Nesse sentido, um dos pontos mais alarmantes discutidos pelo estudo é a “socialização pela violência”. Segundo Paiva (2019), para os jovens das periferias de Fortaleza, a violência não é um evento extraordinário, mas um elemento constituinte de sua formação. O Estado, por sua vez, falha ao se apresentar apenas como braço repressivo e nunca como garantidor de direitos (Oliveira Silva Filho; Mariano, 2020), permitindo o florescimento de instâncias alternativas de regulação social. Ademais, o racismo estrutural e a discriminação institucional compõem a base dessa dinâmica de dominação e sujeição “contra os classificados como indesejáveis” (Paiva, 2019, p. 181). O autor destaca que a atuação das agências de segurança e do sistema de justiça, que destinam às populações negras e periféricas um tratamento pautado pela suspeição e pelo controle repressivo, reitera o isolamento social dessas comunidades, validando a percepção de que o Estado exerce prioritariamente uma função punitiva e segregadora. Consequentemente, os coletivos criminais encontraram no Ceará, sobretudo a partir dos anos 2010, um terreno fértil para exercer o papel de provedores de uma ordem interna, baseada em códigos próprios que preenchem a carência de proteção estatal. O estudo conclui que a configuração atual do crime em Fortaleza é o resultado de uma convergência entre a retirada estratégica do Estado das garantias sociais, a reprodução de preconceitos raciais nas instâncias de poder e a capacidade organizativa de grupos que transformaram a violência em um instrumento de governança política e territorial.

⁴⁰ *Bulk surveillance*, ou vigilância em massa, corresponde à coleta e ao armazenamento sistemáticos, automatizados e indiscriminados de dados de comunicação de uma grande parte ou da totalidade de uma população. Essa modalidade de monitoramento funciona como uma rede de arrasto que captura informações para análise posterior, sem que haja uma suspeita prévia contra indivíduos específicos. Por não discriminar cidadãos comuns de potenciais infratores, essa prática é amplamente questionada devido ao seu potencial de violar o direito fundamental à privacidade (Murray; Fussey, 2019).

tecnológico tende a, em médio e longo prazo, aprofundar desigualdades, na medida em que intensifica a negação de direitos a uma parte importante da população (Santaella, 2025, p. 13).

Por meio da análise crítica do discurso, Barreto e Ferreira (2023) apontam que as campanhas publicitárias no campo da segurança pública cearense frequentemente estabelecem um vínculo direto entre a garantia de paz e ordenação coletiva e a união de força física tradicional e inteligência artificial (Melo; Serra, 2022; Morozov; Bria, 2019), no intuito de estimular a aceitação social de medidas de controle invasivas. As autoras analisam como a Nova Estratégia de Segurança Pública (NESP) fomentou a reestruturação das táticas de policiamento no Ceará, ao apresentar ferramentas tecnológicas como respostas definitivas para os desafios históricos enfrentados pela segurança pública estadual.

De modo geral, o argumento governamental atribui à tecnologia a capacidade de conferir maior racionalidade e tecnicidade às práticas policiais, apresentando-a como instrumento apto a reduzir a margem de subjetividade nas abordagens e a ampliar a eficiência estatal no campo da segurança pública. Essa formulação ancora-se na ideia de que os aparatos algorítmicos atuam como multiplicadores de inteligência, promessa que visa dissociar esses recursos da imagem de uma vigilância autoritária (Lins, 2020; Barreto; Ferreira, 2023). Nesse contexto, a tecnologia seria capaz de expandir os horizontes das políticas punitivas, ao permitir que o Estado se torne mais eficiente do que o crime (Campello, 2021; Duarte, 2024).⁴¹

⁴¹ A compreensão desse discurso exige a consideração dos *standards* de prova que norteiam a atividade policial e judicial no Brasil. *Standards* (Matida, 2018; Ferrer-Beltrán, 2022; Vasconcellos, 2020) são parâmetros normativos que indicam os níveis mínimos de justificativa, razoabilidade ou evidência necessários à formação de determinado convencimento. Eles funcionam como critérios de racionalidade e proporcionalidade, delimitando a atuação estatal diante de situações concretas que exigem avaliação contextual, a fim de evitar decisões arbitrárias e promover coerência na aplicação da lei. No processo penal e na atividade policial, a suspeita constitui um dos *standards* probatórios mais relevantes para a legitimação de determinadas medidas investigativas, sendo responsável por condicionar a abordagem, a busca pessoal e outras formas de interferência à existência de elementos concretos, verificáveis e vinculados à situação analisada. Esse requisito assume especial importância em contextos nos quais determinados corpos, territórios e modos de agir são historicamente associados à criminalidade. Quando o discurso governamental afirma que recursos algorítmicos tornam a abordagem policial mais técnica e racional, ele atribui a esses sistemas a capacidade de preencher o conteúdo dos *standards* jurídicos com maior objetividade. A racionalidade jurídica dos *standards*, contudo, exige fundamentação inteligível e possibilidade de controle posterior. Por essa razão, a utilização de sistemas algorítmicos em abordagens, identificações ou prisões demanda a compreensão dos dados empregados, dos critérios de classificação, das margens de erro admitidas e das circunstâncias concretas que justificaram a intervenção, uma vez que a legalidade da medida depende da reconstrução do caminho decisório que conduziu à interferência estatal. Soma-se a esse quadro a incidência do tirocínio policial (Schlittler, 2016), entendido como a percepção empírica e subjetiva do agente de segurança, uma habilidade desenvolvida pela prática cotidiana que, embora essencial à atividade investigativa, frequentemente colide com os limites impostos pelo Estado de Direito. Isso porque a experiência policial, isoladamente considerada, não fornece os elementos essenciais para reconstruir o raciocínio que levou à abordagem, à busca ou à prisão. Essa limitação se intensifica quando o tirocínio está associado a sistemas algorítmicos, visto que ambos podem incorporar padrões de seletividade penal, sobretudo quando a experiência policial se forma em territórios

Barreto e Ferreira (2023) concluem que o destaque conferido ao fator tecnológico, seja em propostas eleitorais, seja em campanhas políticas de governos já eleitos, resulta na fixação de um paradigma de controle social estruturado pela combinação entre um sentimento de insegurança generalizado e a legítima expectativa de uma solução técnica e definitiva para os desafios inerentes à segurança pública no território cearense (Barreto; Ferreira, 2023). Esse fenômeno demonstra como a percepção de perigo iminente facilita a aceitação de métodos de monitoramento que, em períodos de estabilidade social, enfrentariam maior escrutínio quanto à sua proporcionalidade e impacto na privacidade dos indivíduos.

No entanto, esse discurso oculta as falhas técnicas e os erros cometidos pelos sistemas, bem como os danos colaterais e as violações de direitos que acompanham sua implementação. A urgência fabricada pelo pânico em torno da criminalidade funciona, assim, como um escudo que impede o debate público sobre os limites da vigilância em massa – tema que será aprofundado na seção seguinte.

4.3 Etiquetamento, seletividade penal e racialização do controle no contexto cearense

A incorporação de tecnologias de reconhecimento facial às políticas públicas de segurança insere-se em um campo social estruturado por mecanismos históricos de estigmatização e controle (Duarte; Nunes; Lima, 2023). Nesse sentido, a teoria do etiquetamento, ou *labelling approach* (Becker, 2008; Goffman, 1981; Lemert, 1967), permite compreender as dinâmicas que fundamentam a reação social ao desvio. A teoria sustenta que a criminalidade não é uma característica intrínseca ao ato desviante, mas sim o resultado de um processo de interação social (Aguiar, 2021; Dieter, 2012). A distinção entre “delinquentes” e “cidadãos comuns” situa-se, então, na aplicação de rótulos e estigmas pelas instâncias de controle social (Aguiar, 2021), que contribuem para a consolidação de carreiras criminosas (Becker, 2008; Dieter, 2012; Aguiar, 2021).

Becker (2008) enfatiza que os grupos sociais produzem o desvio ao estabelecer normas e ao aplicá-las seletivamente a sujeitos específicos. De acordo com o autor, esse processo de rotulação possui efeitos concretos na trajetória dos indivíduos, na medida em que altera sua identidade pública e reorganiza suas possibilidades de inserção comunitária ao restringir o acesso a circuitos legítimos de sociabilidade, o que intensifica processos de

marcados pela desigualdade racial e pela criminalização da pobreza, ou quando a base de dados utilizada na tomada de decisão foi construída a partir dessas mesmas práticas seletivas.

marginalização (Becker, 2008, p. 44). Dessa maneira, “tratar uma pessoa como se ela fosse em geral, e não em particular, desviante, produz uma profecia autorrealizadora” (Becker, 2008, p. 44), uma vez que o ciclo de rotulação influencia a *psique* (Han, 2018) dos indivíduos, podendo induzi-los a internalizar a identidade criminal. Como consequência, criam-se condições para a ocorrência da delinquência secundária⁴² (Dieter, 2012; Lemert, 1967), entendida como o comportamento delitivo decorrente da estigmatização social.

A aplicação dessas premissas ao contexto da segurança pública revela que o sistema de justiça tende a privilegiar a punição de determinados grupos sociais em razão de sua visibilidade e vulnerabilidade (Aguar, 2021; Dieter, 2012). Nessa perspectiva, o estigma (Goffman, 1981) atua como marcador social que legitima práticas diferenciadas de controle e sustenta a suspensão de garantias fundamentais. No contexto brasileiro, esses processos encontram fundamento em uma estrutura marcada pela herança colonial e escravocrata, que institui a população negra e periférica como destinatária preferencial das práticas de controle e repressão estatal (Almeida, 2019; Carneiro, 2023; Corrêa, 2021; Flauzina, 2006; Melo; Serra, 2022; Moreira, 2020; Nunes *et al.*, 2025; Ramos *et al.*, 2022; Reis *et al.*, 2021; Seyferth, 2002; Silva, 2024; Silva; Silva, 2019).

A contribuição de Misse (1999; 2006; 2008; 2009; 2010) aprofunda essa análise ao expandir as fronteiras da teoria do etiquetamento e adaptá-la às especificidades da realidade brasileira. O autor introduz o conceito de sujeição criminal, definida como um processo social de constituição de subjetividades e identidades no qual o crime corresponde a um atributo ontológico do sujeito. Trata-se, portanto, de uma construção de tipos sociais⁴³ propensos à prática criminosa, fundamentada na interpretação e no enquadramento de determinados eventos e locais em categorias de criminalização previamente estabelecidas (Misse, 1999; 2006; 2010).

Esse processo territorializa-se nas periferias, atingindo, inclusive, crianças e adolescentes, cujas vidas são precocemente marcadas pela estigmatização de seus corpos e pela expectativa social de um destino criminal (Ramos *et al.*, 2022; Reis *et al.*, 2021; Silva, 2024;

⁴² De acordo com Lemert (1967), o desvio primário refere-se a comportamentos que, embora transgressores, possuem causas variadas e não alteram a estrutura psíquica ou o papel social do agente. A transição para o desvio secundário ocorre quando a reação social ao ato inicial provoca uma reorganização da identidade do sujeito, que passa a utilizar seu comportamento desviante como um meio de defesa ou adaptação aos problemas criados pela reação social.

⁴³ Dentre as categorias sociais abordadas por Misse (2006), a figura do “bandido” representa um tipo social sobre o qual recaem os sentimentos morais mais repulsivos da sociedade. O bandido é o alvo preferencial de ações estatais que ignoram os limites da legalidade, sendo frequentemente associado a indivíduos marcados pela pobreza, pela cor da pele e por um estilo de vida periférico.

Silva; Silva, 2019). O Conselho Nacional de Justiça (CNJ), atento a essas distorções, instituiu, por meio da Portaria nº 209, de 31 de agosto de 2021, o *Grupo de Trabalho Reconhecimento de Pessoas*, com a finalidade de “estudar e elaborar propostas para o reconhecimento pessoal em processos criminais e sua aplicação no âmbito do Poder Judiciário, com o objetivo fundamental de evitar a condenação de pessoas inocentes” (Conselho Nacional de Justiça, 2022, p. 13).

O relatório salientou que o Brasil não é capaz de dissociar a criminalização da repressão racial, de modo que “a luta contra o erro de reconhecimento é, fundamentalmente, parte do tardio esforço das autoridades públicas para diminuição do racismo que se expressa e se estrutura por meio da seletividade penal” (Conselho Nacional de Justiça, 2022, p. 15). Dentre os principais obstáculos enfrentados pelos pesquisadores, a precariedade das informações disponíveis sobre a utilização de tecnologias de reconhecimento facial no país é um dos fatores que mais dificulta a construção de diagnósticos precisos e a “proposição de medidas institucionais destinadas ao monitoramento dos processos de implementação e gestão desses sistemas e ao tratamento dos dados biométricos coletados” (Conselho Nacional de Justiça, 2022, p. 41-42).

De acordo com o comitê técnico, somente os membros do Ministério Público de São Paulo, Santa Catarina, Mato Grosso do Sul e Goiás forneceram dados consistentes quando perguntados sobre a existência de sistemas de reconhecimento facial em suas unidades federativas. Os demais estados, inclusive o Ceará, deram “respostas genéricas sem a possibilidade de identificação do sistema em vigor” (Conselho Nacional de Justiça, 2022, p. 41-42).

Ademais, o documento evidencia que tecnologias de reconhecimento facial ampliam a escala de erros já presentes em métodos tradicionais, especialmente contra pessoas negras (Conselho Nacional de Justiça, 2022, p. 41-44). Segundo o comitê, “se os reconhecimentos fotográficos e pessoais já se demonstram com alto grau de falibilidade, as tecnologias e algoritmos que possuem esse intuito escancaram e ampliam a escala de possibilidade de erros e violações de direitos” (Conselho Nacional de Justiça, 2022, p. 41), uma vez que se concentram em características físicas.

Em razão do elevado grau de falhas, o grupo ressalta que diversas localidades ao redor do mundo aboliram ou restringiram o uso do reconhecimento facial devido a

preocupações com a violação de direitos fundamentais e liberdades individuais, enfatizando “o potencial dessa tecnologia para agravar problemas crônicos do sistema de justiça criminal como o perfilamento racial e os falsos reconhecimentos, ambos fatores catalisadores da prisão e/ou condenação de pessoas inocentes” (Conselho Nacional de Justiça, 2022, p. 41-42). Os pesquisadores apontam a ocorrência de vieses que, desde a origem, produzem distorções nos resultados da operacionalização dos algoritmos biométricos como uma das razões para a imposição de limitações sobre o uso da tecnologia. Nessa toada:

Nenhum software de reconhecimento facial desenvolvido até o momento goza de 100% de precisão. Os falsos positivos, que ocorrem quando o sistema de reconhecimento facial identifica, de maneira errônea, duas pessoas distintas, são inerentes ao uso dessa tecnologia e não podem ser considerados um efeito colateral de menor importância da sua implementação, dado que a partir de um falso positivo pessoas podem ser submetidas por agentes de segurança a constrangimentos e abusos que podem resultar em graves e, por vezes, irreversíveis, violações de direitos humanos. Ademais, a seletividade racial presente no funcionamento do sistema de justiça criminal brasileiro determina a sobre representação de pessoas negras no universo de investigados, processados, condenados e encarcerados, motivo pelo qual os bancos de dados que costumam ser empregados localmente para subsidiar o funcionamento dos softwares de reconhecimento facial – de pessoas com antecedentes criminais ou procuradas pela justiça, por exemplo – são compostos por pessoas majoritariamente negras, fator que potencializa os riscos de falsos positivos e de criminalização em relação a este grupo, em um grave círculo de reprodução e agravamento do racismo e da discriminação racial (Conselho Nacional de Justiça, 2022, p. 43-44).

No Ceará, essas dinâmicas manifestam-se de forma particularmente intensa. Dados indicam que, de um total de 21.457 pessoas encarceradas em novembro de 2025, cerca de 18.664 se autodeclaram pretas ou pardas, representando cerca de 87% da população prisional do estado (Leite, 2025). Essa sobre-representação é acompanhada por uma incidência desproporcional de mortes violentas, em uma expressão da necropolítica⁴⁴ (Mbembe, 2018) vigente no estado. Segundo dados do Atlas da Violência 2025 (Cerqueira; Bueno, 2025, p. 76), no Ceará, a letalidade possui um recorte racial bem definido, concentrando-se principalmente em corpos negros: cerca de 39,8% das vítimas de homicídio no estado em 2023 foram pessoas negras.

⁴⁴ O conceito de necropolítica descreve a capacidade de estabelecer parâmetros que subordinam a vida ao poder da morte. Diferentemente da biopolítica tradicional (Foucault, 1999; 2005), que se ocupa da otimização da vida, Mbembe (2018) sustenta que a necropolítica se dedica à administração da morte. Segundo o autor, essa gestão não se limita à promoção de assassinatos diretos, abrangendo também a criação de zonas de “não-vida”, caracterizadas por um estado de exceção permanente, no qual corpos são expostos a condições precárias de existência. Nesse contexto, a soberania estatal manifesta-se primordialmente como o direito de matar, sendo a necropolítica a forma contemporânea de exercício do poder voltada à destruição de corpos considerados indesejáveis ou perigosos para a preservação de outros. Em cenários necropolíticos, corpos negros e de grupos vulneráveis são privados de direitos e submetidos à violência arbitrária do Estado.

Em 2021, o relatório *Pele Alvo: a cor que a polícia apaga* (Ramos *et al.*, 2022, p. 7), elaborado pela Rede de Observatórios da Segurança, mostrou que 92,3% das pessoas mortas em ações policiais no Ceará, nos casos onde houve identificação racial, eram negras. O documento também chamou atenção para uma estratégia de ocultamento do racismo institucional presente nas forças de segurança cearenses, ao sublinhar que 69% dos registros de mortes decorrentes de intervenção policial não possuíam informações sobre a raça das vítimas (Ramos *et al.*, 2022, p. 9). A análise realçou, ainda, que a distribuição espacial da letalidade policial em Fortaleza é racializada e classista. De acordo com o levantamento, naquele ano, as maiores taxas de mortes por intervenção estatal estiveram concentradas em bairros pobres e periféricos, como Cajazeiras, Parque Araxá, Benfica, Mondubim e Curió (Ramos *et al.*, 2022, p. 13).

Em 2023, a seletividade racial na atuação das forças de segurança cearenses permaneceu acentuada. Segundo o relatório *Pele alvo: mortes que revelam um padrão* (Ramos *et al.*, 2024, p. 18), naquele ano, o número de pessoas negras mortas em decorrência da letalidade policial foi oito vezes superior ao de pessoas brancas. Desde 2019, o estado contabilizou 894 vítimas de intervenção estatal, sendo 189 apenas no ano de 2024 (Ramos *et al.*, 2025, p. 24). Os dados mais recentes também destacam a persistência da subnotificação racial nesse período: em 51,3% das ocorrências não havia informação sobre a raça das vítimas. Entre os casos em que essa informação foi registrada, 79,3% eram negros (Ramos *et al.*, 2025, p. 24).

A incorporação de sistemas de reconhecimento facial nesse contexto tende a replicar e exacerbar as dinâmicas de seletividade penal, inclusive com o aumento de abordagens policiais indevidas e o encarceramento em massa de populações vulneráveis, uma vez que os *softwares* são alimentados por dados que espelham o viés racial das investigações e prisões anteriores (Conselho Nacional de Justiça, 2022; O’Neil, 2017; Brayne, 2021). Esse fenômeno foi corroborado logo nos meses iniciais de expansão dessas tecnologias no Brasil: entre junho e outubro de 2019, aproximadamente 90,5% das prisões efetuadas mediante o emprego de algoritmos biométricos recaíram sobre indivíduos negros (Nunes, 2019, p. 69).

Alinhada a essa evidência, a Recomendação Geral nº 36, publicada em novembro de 2020 pelo Comitê para a Eliminação da Discriminação Racial (CERD) da Organização das Nações Unidas (ONU), adverte que o crescente uso de algoritmos, inteligência artificial e reconhecimento facial pelas forças de segurança pública potencializa o risco de

aprofundamento do racismo, da xenofobia e da discriminação racial, culminando na violação de direitos humanos e fundamentais. Segundo o CERD (2020), a utilização de registros criminais pretéritos para subsidiar os bancos de dados de algoritmos inteligentes pode viabilizar o recrudescimento da vigilância e do controle sobre grupos historicamente vulnerabilizados pelas estatísticas criminais – notadamente a população negra –, cristalizando e retroalimentando práticas discriminatórias.

Alguns episódios ocorridos no Ceará exemplificam a materialização dessas dinâmicas. O primeiro deles ocorreu em 2021, com a inclusão de uma fotografia do ator estadunidense Michael B. Jordan no Termo de Reconhecimento Fotográfico da Polícia Civil do Ceará (PCCE), utilizado nas investigações relativas à chacina da Sapiranga, evento que vitimou cinco pessoas em Fortaleza (Foto..., 2022; Cruz, 2022). A presença de uma figura pública internacional em um contexto de identificação de suspeitos locais ilustra a fragilidade dos critérios empregados pelas forças de segurança do estado, muitas vezes preenchidos por uma única característica comum: o perfil racial que mais se aproxima do imaginário de criminalidade construído socialmente (Souza; Ribeiro; Banchik, 2026; Cruz, 2022).

Outro exemplo relevante encontra-se no uso do reconhecimento facial na Arena Castelão (Ceará, 2025b). A iniciativa – articulada pela SSPDS-CE, em cooperação com a Empresa de Tecnologia do Ceará (Etice) e a Secretaria de Esportes (Sesporte) – visa a captura de indivíduos com mandados de prisão em aberto, mediante a integração entre o sistema de monitoramento do estádio e o Banco Nacional de Mandados de Prisão (Silva; Xavier, 2025; Castro, 2025). Todavia, a obrigatoriedade do cadastramento biométrico como condição para o ingresso no recinto implica a utilização de informações sensíveis pertencentes a cidadãos sobre os quais não recai qualquer suspeição específica. Consequentemente, institui-se um regime de vigilância indistinta sobre todos aqueles que transitam pelo local, o que sedimenta uma relação de desconfiança generalizada entre o Estado e a sociedade civil, em virtude da mitigação das garantias fundamentais à privacidade e à intimidade (Silva; Xavier, 2025).

Por fim, outro episódio que evidenciou falhas nos sistemas de reconhecimento facial no Ceará envolveu a empresa IPQ Tecnologia, incumbida da manutenção de aproximadamente 513 pontos de videomonitoramento no estado (Luz, 2026). Conforme relatos, os sistemas operacionalizados pela entidade já confundiram seres humanos com sacos de lixo e outros objetos inanimados. Malgrado a empresa sustente que sua tecnologia possui um índice de precisão superior a 86%, o evento demonstra a fragilidade dessa métrica, dado o elevado

número de falsos positivos sob condições ambientais ordinárias de iluminação e angulação (Luz, 2026).

É particularmente significativo que o erro – a associação entre um rosto humano e um saco de lixo – tenha ocorrido contra uma pessoa negra (Luz, 2026). Tal situação, além de expor a insuficiência técnica do sistema, evidencia a reprodução de estigmas sociais historicamente dirigidos a corpos negros no estado do Ceará. Essa constatação conduz à necessidade de examinar os limites normativos que regulam o uso das tecnologias de reconhecimento facial, especialmente no que se refere à proteção de dados pessoais e à garantia de direitos fundamentais, tema que será desenvolvido no tópico seguinte.

4.4 LGPD, segurança pública e os limites do reconhecimento facial

A promulgação da Lei nº 13.709/2018 instituiu, no ordenamento jurídico nacional, um regime voltado à tutela dos dados pessoais, posteriormente elevado ao patamar de direito fundamental pela Emenda Constitucional nº 115/2022 (Brasil, 2022a). Esse microsistema legislativo fixou princípios estruturantes que conduzem o tratamento de informações sensíveis, bem como delimitam o exercício do poder informacional por agentes públicos e privados (Souza; Viola; Padrão, 2019; Pinheiro, 2020; Frazão, 2021).

Todavia, a implementação dessa norma encontra resistência significativa no âmbito interno. Os controladores (Souza; Viola; Padrão, 2019; Bucar; Viola, 2020) – pessoas físicas ou jurídicas que detêm competência para a tomada de decisões sobre o tratamento de dados pessoais, conforme exegese do artigo 5º, inciso VI, da LGPD (Brasil, 2018) – tendem a assimilar os imperativos legais como meros entraves burocráticos ao desenvolvimento de suas atividades (Pinheiro, 2020). Essa postura dificulta a consolidação de uma cultura corporativa orientada à preservação de dados pessoais, o que, por conseguinte, compromete a eficácia da tutela jurídica conferida aos titulares dessas informações (Souza; Viola; Padrão, 2019).

Nesse panorama, Mendes e Fonseca (2020) ressaltam o risco de que o instituto do legítimo interesse do controlador (Souza; Viola; Padrão, 2019; Bucar; Viola, 2020) – hipótese prevista no artigo 7º, inciso IX, da LGPD, que admite o tratamento de dados pessoais independentemente de anuência prévia – seja manejado como uma cláusula geral de validação para processamentos realizados à revelia da vontade do titular. Sob esse prisma, o critério da necessidade atua como um mecanismo imprescindível de contenção de abusos jurídicos, impondo a obrigatoriedade de um rigoroso controle de legalidade e o estabelecimento de

finalidades legítimas e compatíveis com as expectativas do titular (Santana, 2022).

No contexto da segurança pública e da persecução penal, a introdução de sistemas de identificação biométrica acentua uma das tensões mais sensíveis do constitucionalismo contemporâneo: a colisão entre direitos fundamentais. De um lado, situa-se o direito à proteção de dados pessoais, cuja função precípua consiste em assegurar ao indivíduo algum grau de domínio sobre as informações que compõem sua identidade física, social e digital (Rodotà, 2008). De outro, o direito à segurança pública, disposto no artigo 144 da Constituição Federal (Brasil, 1988), concebido como dever do Estado e prerrogativa coletiva indispensável à manutenção da ordem democrática. Longe de configurarem grandezas harmoniosas, o tensionamento entre esses dois vetores atinge seu ápice quando o aparato repressivo estatal reivindica o monitoramento biométrico como condição de eficiência operacional.

À luz da teoria dos direitos fundamentais, notadamente a metodologia do sopesamento formulada por Alexy (2008), sabe-se que os direitos em rota de colisão possuem a natureza de mandamentos de otimização. Isso exige que sua aplicação ocorra na maior medida possível, sopesadas as possibilidades fáticas e jurídicas do caso concreto. Todavia, a retórica securitária contemporânea tende a atribuir à segurança pública um caráter absoluto, capaz de justificar o esvaziamento reflexo das liberdades individuais. Essa leitura aproxima-se de uma lógica de “jogo de soma zero”⁴⁵ (Shubik, 1992; Von Neumann; Morgenstern, 1953) – que pressupõe o sacrifício de parcelas de liberdade em prol de supostos incrementos de segurança –, perspectiva que desnatura a essência do Estado Democrático de Direito.

Sob essa ótica, a invocação abstrata da proteção social não basta para legitimar intervenções estatais irrestritas, visto que sua finalidade última é, precisamente, garantir o livre exercício dos direitos fundamentais. A partir de sua vertente objetiva, tais direitos irradiam ao poder público o dever de criação de condições normativas e institucionais adequadas ao seu exercício (Sarlet, 2012). Nesse sentido, a proteção de dados assume função estruturante para a ordem jurídica, pois baliza a capacidade de coleta de dados conferida ao Estado (Rodotà, 2008). Por esse motivo, a restrição ao direito à proteção de dados decorrente do uso de tecnologias biométricas exige uma filtragem constitucional rigorosa, pautada pelo princípio da proporcionalidade em sua tríplice dimensão: adequação, necessidade e proporcionalidade em

⁴⁵ O conceito de jogo de soma zero tem origem na Teoria dos Jogos (Von Neumann; Morgenstern, 1953) e descreve uma situação em que o ganho de um participante é necessariamente equivalente à derrota do oponente, o que impossibilita a criação de uma solução em que ambas as partes sejam vitoriosas.

sentido estrito.

No plano da adequação, impõe-se avaliar se o reconhecimento facial constitui um meio idôneo para atingir os fins propostos pelo Estado. Não basta, portanto, invocar genericamente a eficiência investigativa, fazendo-se necessária a comprovação de que o sistema empregado apresenta desempenho satisfatório em relação aos diferentes grupos populacionais submetidos à vigilância. Em contextos marcados por seletividade penal e desigualdade racial, a aferição da idoneidade do meio deve considerar, ainda, a incidência desproporcional de falsos positivos sobre pessoas negras e outros grupos historicamente vulnerabilizados (Buolamwini; Gebru, 2018; Grother; Ngan; Hanaoka, 2019; Silva, 2024).

Quanto à necessidade, deve-se verificar a existência de meios alternativos igualmente eficazes para a persecução penal, mas que impliquem menor grau de ingerência na esfera íntima dos cidadãos. Essa conclusão se justifica na medida em que a generalização promovida pela vigilância biométrica rompe com o padrão (*standard*) tradicional do processo penal democrático, o qual exige a individualização da suspeita fundada em elementos objetivos, conforme discutido anteriormente (Matida, 2018; Ferrer-Beltrán, 2022; Vasconcellos, 2020).

Por seu turno, a proporcionalidade em sentido estrito requer a ponderação entre o eventual acréscimo de eficiência estatal e a intensidade da restrição imposta aos direitos fundamentais. Nesse exame, o eventual incremento da atividade policial deve ser confrontado com a amplitude da vigilância instituída, a sensibilidade dos dados tratados e a possibilidade de discriminação racial (Buolamwini; Gebru, 2018). No caso do reconhecimento facial, a proporcionalidade deve ser aferida a partir de múltiplos parâmetros jurídicos, uma vez que a superexposição dos traços biológicos de um indivíduo atinge o núcleo essencial do direito à dignidade humana em face das assimetrias de poder informacional existentes na relação entre cidadão e Estado.

Nessa perspectiva, o sopesamento constitucional exige que a introdução de ferramentas de vigilância biométrica na atividade persecutória penal seja condicionada a uma densa regulação legal, com a incorporação do princípio da precaução como eixo normativo (Bioni; Luciano, 2019) e a instituição de uma governança de dados fundada em avaliações prévias de impacto, supervisão humana qualificada, auditorias periódicas e independentes, além de mecanismos de revisão e contestação das decisões automatizadas. Ausentes essas salvaguardas, o sacrifício imposto à liberdade, à igualdade racial e à autodeterminação

informativa tende a superar o benefício público alegadamente produzido pelas medidas de monitoramento biométrico.

No entanto, o manejo de informações pessoais na seara investigativa e persecutória constitui uma das áreas de maior complexidade e carência regulatória no país (Lima; Fonsêca, 2025). Um dos principais desafios enfrentados pelo ordenamento jurídico brasileiro reside na harmonização entre os postulados de transparência administrativa e intimidade (Canhadas, 2020; Ribeiro, 2020). Nesse cenário, o debate acerca do consentimento demanda dos agentes públicos e privados uma assimilação proativa da lógica de prevenção e segurança que estrutura o regime normativo estabelecido pela LGPD.

Segundo a perspectiva de Bioni (2020), o consentimento fundamenta-se na prerrogativa do titular de exercer o controle sobre a destinação de suas informações. A legitimidade desse ato decisório está atrelada à presença de uma manifestação de vontade livre, informada e vinculada a finalidades determinadas. Essa exigência adquire especial relevância quando analisada no contexto do reconhecimento facial, uma vez que, como demonstrado no capítulo anterior, a coleta indiscriminada de informações biométricas – classificadas como dados pessoais sensíveis pelo artigo 5º, inciso II, da LGPD (Brasil, 2018) – estende o processamento de dados para além dos sujeitos submetidos a procedimentos investigativos específicos (Nunes, 2019; Duarte; Nunes; Lima, 2023; Martins *et al.*, 2024).

Nessa toada, a exclusão das atividades de segurança pública do escopo de aplicação da LGPD, conforme estabelecido pelo artigo 4º, inciso III, alíneas “a” e “d”, da referida legislação (Brasil, 2018), permite que o tratamento de dados biométricos ocorra à margem dos requisitos de consentimento e transparência aplicáveis às relações privadas (Azevedo *et al.*, 2022; Silva, 2025b). Essa restrição – que remete o tratamento de dados à legislação específica ainda inexistente, nos termos do artigo 4º, §1º (Brasil, 2018) – instaura uma lacuna normativa que amplia a discricionariedade governamental e dificulta a fixação de parâmetros materiais de controle sobre a atuação estatal (Nunes, 2019; Duarte; Nunes; Lima, 2023; Martins *et al.*, 2024).

De acordo com Frazão (2021), a ausência desses mecanismos de gerenciamento compromete a racionalidade preventiva que fundamenta a própria LGPD, sobretudo no que se refere à ideia de *privacy by design*,⁴⁶ estipulada no artigo 46, §2º, do referido diploma legal

⁴⁶ Essa diretriz exige que os princípios de segurança, sigilo, prevenção de danos e avaliação de riscos sejam considerados desde o desenho do produto ou serviço até a sua efetiva execução (Frazão, 2021).

(Brasil, 2018). Em virtude dessa defasagem, a inércia legislativa enfraquece os deveres de prevenção e mitigação de danos, favorecendo a implementação de tecnologias de alto risco antes da estruturação de salvaguardas proporcionais à sua magnitude (Lima; Fonsêca, 2025).

A questão torna-se ainda mais sensível diante do racismo estrutural (Almeida, 2019; Moreira, 2020) que atravessa as instituições, práticas e ferramentas de segurança pública, a exemplo do reconhecimento facial (Conselho Nacional de Justiça, 2022; Nunes, 2019; Ramos *et al.*, 2022; 2024; 2025; Duarte; Nunes; Lima, 2023; Martins *et al.*, 2024; Buolamwini; Gebru, 2018; Benjamin, 2019). Como visto anteriormente, a utilização desses sistemas em contextos caracterizados pela seletividade penal potencializa os riscos de criminalização da negritude, circunstância que torna imprescindível a fixação de controles jurídicos especializados, adequados à natureza sensível dos dados processados e à gravidade dos efeitos produzidos sobre populações historicamente vulnerabilizadas (Nunes, 2019; Duarte; Nunes; Lima, 2023; Martins *et al.*, 2024).

A participação de pessoas jurídicas de direito privado acentua a complexidade dessa problemática. O parágrafo segundo do artigo 4º da LGPD (Brasil, 2018) estabelece condicionantes à atuação de particulares no processamento de dados para fins de segurança pública, admitindo sua participação somente sob a tutela de entes públicos. Por sua vez, o parágrafo quarto do mesmo artigo impõe limites à transferência integral de bases de dados à iniciativa privada. Apesar dessas disposições, a realidade fática demonstra a concentração de dados sensíveis sob a custódia de organizações particulares, como a IPQ Tecnologia (Luz, 2026), circunstância que suscita questionamentos acerca da efetividade da fiscalização estatal sobre esses repositórios (Duarte; Nunes; Lima, 2023; Martins *et al.*, 2024).

Nesse cenário, evidencia-se a imperatividade de um dever de cuidado rigoroso atribuído aos agentes privados, os quais devem assegurar padrões elevados de segurança, diligência e mitigação de riscos a direitos fundamentais (Frazão, 2021). Por essa razão, a fim de suprir a lacuna legislativa identificada, iniciou-se um movimento direcionado à elaboração de propostas para a criação de uma “LGPD Penal” (Fernandes; Resende, 2023; Azevedo *et al.*, 2022).

Em 2019, a Câmara dos Deputados instituiu uma comissão de juristas com o intuito de desenvolver um anteprojeto de lei voltado à disciplina do tratamento de dados pessoais em atividades de segurança pública e persecução penal (Azevedo *et al.*, 2022). O texto originário

propunha a observância de axiomas como a proporcionalidade, a legalidade e a transparência, além de estipular a obrigatoriedade de relatórios de impacto e a implementação de instrumentos de controle institucional e social sobre o uso de tecnologias de vigilância. Essas previsões objetivavam assegurar uma supervisão qualificada sobre os sistemas de inteligência artificial empregados pelo Estado, estabelecendo balizas fundamentais de acurácia, responsabilidade e governança (Azevedo *et al.*, 2022).

Um dos desdobramentos dessas articulações consistiu na propositura do Projeto de Lei nº 1515/2022 (Brasil, 2022b), o qual introduziu modificações substanciais em comparação ao anteprojeto precedente. Avaliações conduzidas por organizações independentes, a exemplo do Laboratório de Políticas Públicas e Internet (LAPIN), indicam que a referida proposta expande excessivamente as bases legais destinadas ao processamento de dados (Azevedo *et al.*, 2022, p. 3-4) e reduz a amplitude das garantias conferidas aos titulares (Azevedo *et al.*, 2022, p. 22). O texto também promove a supressão dos princípios da transparência e do livre acesso (Azevedo *et al.*, 2022, p. 24), além da autodeterminação informativa (Rodotà, 2008) e da responsabilidade (Azevedo *et al.*, 2022, p. 7-8), conceitos essenciais à gestão de dados pessoais. Simultaneamente, a proposição amplia o poder discricionário do Estado na administração de bancos de dados biométricos (Azevedo *et al.*, 2022, p. 28), o que acentua a opacidade dos sistemas empregados na segurança pública.

Conforme exposto, essa questão adquire contornos de maior gravidade em face da implementação de tecnologias de vigilância ostensiva, notadamente o reconhecimento facial, que viabiliza o processamento ininterrupto de dados biométricos em logradouros públicos (Nunes *et al.*, 2025; Rosa *et al.*, 2025). Segundo as deliberações do Grupo de Trabalho “Reconhecimento de Pessoas”, a captura indiscriminada de características sensíveis pode condicionar o comportamento social e restringir o exercício de prerrogativas fundamentais, tais como o direito de locomoção, a liberdade de manifestação e o direito de reunião (Conselho Nacional de Justiça, 2022, p. 43-44).

Dada a gravidade de tais implicações, e enquanto a lacuna legislativa subsiste, o Ministério da Justiça e Segurança Pública editou a Portaria nº 961/2025 (Brasil, 2025), direcionada ao emprego de tecnologias em procedimentos de investigação criminal e inteligência, visando conferir determinado grau de proteção aos dados pessoais e ao direito à privacidade. Todavia, os atos administrativos possuem alcance limitado frente à necessidade de disciplinar restrições a direitos fundamentais, competências de natureza processual penal,

critérios de auditoria e ferramentas de responsabilização. Sob essa ótica, a proteção de dados na esfera penal demanda a edição de lei formal, alicerçada no respeito à presunção de inocência e à ampla defesa, de modo que a evolução tecnológica das instituições de segurança seja subordinada a limites democráticos claros (Azevedo *et al.*, 2022).

Ademais, a pluralidade de normas que regulam o ambiente digital produz desafios interpretativos. Acadêmicos como Doneda e Mendes (2018), bem como Ribeiro (2020) e Canhadas (2020), asseveram que a compatibilização entre regimes distintos – tais como os delineados pela LGPD, pelo Marco Civil da Internet e pela Lei de Acesso à Informação (LAI) – exige um esforço hermenêutico pautado pelos critérios de especialidade e de cronologia. Essa necessidade evidencia-se, primordialmente, em situações que requerem o equilíbrio entre o princípio da publicidade administrativa, o sigilo, o dever de guarda de registros e a proteção de dados sensíveis.

Dessa forma, a estruturação de um regime jurídico condizente com o tratamento de informações pessoais no âmbito da segurança pública representa uma condição imperativa para a salvaguarda das garantias constitucionais. Em que pese o cenário brasileiro apresente progressos normativos relevantes, notadamente com a alçada da proteção de dados pessoais à categoria de preceito constitucional e a promulgação da LGPD, as lacunas atinentes à persecução penal, à segurança pública e ao emprego de tecnologias biométricas continuam a comprometer a tutela de direitos e liberdades fundamentais. Por essa razão, a racionalidade preventiva inerente à LGPD deve integrar materialmente a segurança pública. Os imperativos de transparência, auditabilidade e contestabilidade precisam fundamentar todo o ciclo de processamento biométrico, desde a concepção técnica da ferramenta até sua utilização por agentes estatais.

Portanto, a consolidação de um ecossistema robusto de proteção de dados e a articulação entre órgãos públicos, instituições de controle, comunidade científica e sociedade civil são elementos indispensáveis para assegurar que o emprego de tecnologias biométricas guarde compatibilidade com o Estado Democrático de Direito.

5 CONCLUSÃO

O presente trabalho examinou a influência exercida pela opacidade algorítmica, em conjunção com o emprego de dispositivos de reconhecimento facial na esfera da segurança pública, sobre a reprodução de discriminações raciais no estado do Ceará. A investigação foi conduzida por uma abordagem qualitativa, exploratória, descritiva, bibliográfica e documental, orientada pelo método indutivo e estruturada como estudo de caso. A pesquisa iniciou-se a partir da compreensão teórica sobre a sociedade disciplinar e a sociedade de controle, avançando para o exame dos algoritmos, da inteligência artificial, dos vieses cognitivos, da opacidade algorítmica e da responsabilidade por decisões automatizadas. Na sequência, realizou-se a análise situada da infraestrutura de vigilância cearense, com atenção aos riscos sociotécnicos e jurídicos decorrentes da aplicação de sistemas biométricos em contextos marcados pela desigualdade racial.

No primeiro capítulo, o trabalho examinou a sociedade disciplinar como uma forma de organização do poder político. A partir de Foucault (2001), evidenciou-se que as instituições modernas de confinamento, como escolas, fábricas, quartéis, hospitais e prisões, constituíram-se como locais de adestramento e vigilância de corpos indesejáveis. A disciplina foi concebida como uma técnica voltada à produção de sujeitos úteis e dóceis, fundamentada na segmentação do espaço, na hierarquia e no monitoramento contínuo. O panóptico, nesse contexto, foi interpretado como um modelo arquitetônico e político de vigilância, capaz de induzir padrões de comportamento. Esse primeiro movimento permitiu compreender a centralidade do controle dos corpos na formação das instituições modernas e forneceu a base conceitual para a análise das transformações posteriores do poder.

O estudo avançou para a análise da sociedade de controle, sistematizada por Deleuze (1992) como o paradigma estruturante da contemporaneidade. A pesquisa evidenciou que, na sociedade de controle, o exercício do poder se manifesta de maneira contínua e difusa. A concepção do indivíduo disciplinar cedeu espaço à figura do “divíduo”, caracterizado como um sujeito fragmentado em fluxos digitais de informações, métricas e perfis comportamentais. Essa transição possibilitou a observação de um modelo de vigilância estabelecido em domínios abertos e interconectados. A antecipação de riscos, a securitização e a gestão probabilística das ações sociais constituíram os pilares fundamentais desse novo arranjo de poder.

O trabalho investigou, ainda, o uso da tecnologia como instrumento de controle

social. A evolução histórica das modalidades de registro, catalogação e monitoramento demonstrou que os aparatos tecnológicos mantêm uma relação intrínseca com a administração populacional. Os processos de digitalização e datificação intensificaram essa dinâmica, viabilizando o arquivamento, o cruzamento e a análise automatizada de grandes volumes de informações. Nesse horizonte analítico, categorias teóricas como capitalismo de dados, capitalismo de vigilância, sociedade de vigilância, governamentalidade algorítmica e policiamento preditivo foram mobilizadas para demonstrar como os dispositivos tecnológicos ampliam a capacidade de intervenção estatal.

No segundo capítulo, a investigação concentrou-se, a princípio, na delimitação conceitual dos algoritmos. O estudo demonstrou que algoritmos simples seguem sequências finitas e previamente estruturadas de instruções, enquanto modelos complexos utilizam grandes volumes de dados para identificar padrões e produzir inferências estatísticas. Foram analisados conceitos como *big data*, *big analytics*, *machine learning* e *deep learning*. A partir disso, evidenciou-se que a decisão automatizada depende de uma extensa cadeia técnica e de um volumoso acervo informacional, além do estabelecimento de parâmetros, objetivos e critérios de classificação. Essa etapa foi essencial para afastar a compreensão puramente instrumental dos algoritmos e situá-los como estruturas sociotécnicas desenvolvidas em contextos organizacionais específicos.

Posteriormente, a pesquisa avaliou os limites da cognição artificial. A partir da distinção entre inteligência artificial estreita e geral, adotou-se o paradigma da IA fraca como referência para o desenvolvimento do trabalho. O debate entre sintaxe e semântica, sob a ótica de Searle (2006), permitiu compreender que sistemas computacionais manipulam símbolos e padrões estatísticos, sem apreensão genuína de significado. Essa constatação foi relevante para demonstrar que decisões automatizadas dependem da qualidade das bases de dados, das escolhas de modelagem e dos objetivos definidos por agentes humanos responsáveis pela supervisão do sistema.

O trabalho também abordou os vieses, as heurísticas e a transposição de preconceitos ao *design* tecnológico. A princípio, foram analisadas as distorções cognitivas que influenciam decisões humanas, sobretudo em cenários de incerteza e urgência. Em seguida, demonstrou-se que essas tendências podem ser incorporadas aos sistemas computacionais mediante a seleção de variáveis em bases de treinamento, a estipulação de métricas e a escolha dos resultados considerados relevantes. A pesquisa evidenciou que a aparência de neutralidade

técnica pode conferir legitimidade a classificações algorítmicas construídas a partir de dados influenciados por desigualdades históricas.

Ademais, a investigação desenvolveu a noção de racismo algorítmico. Com amparo no referencial teórico de intelectuais como Carneiro (2023), Benjamin (2019) e Silva (2024), o estudo demonstrou que algoritmos podem absorver hierarquias raciais presentes no tecido social e reorganizá-las em processos automatizados de categorização e segregação. No caso das tecnologias de reconhecimento facial, a pesquisa constatou que bases de dados com baixa representatividade, equipes de desenvolvimento pouco diversas e modelos estatísticos treinados em contextos desiguais tendem a produzir resultados desfavoráveis a grupos racializados. O racismo algorítmico foi, assim, compreendido como uma extensão tecnológica da seletividade racial.

A investigação também escrutinou o fenômeno da opacidade algorítmica. A alegoria da caixa-preta serviu como base para a compreensão de sistemas cujo funcionamento interno é inacessível ao escrutínio público. O estudo evidenciou que a opacidade possui dimensões técnicas, estratégicas e cognitivas, decorrentes da complexidade dos modelos, da proteção comercial dos sistemas e da dificuldade de entendimento por parte dos sujeitos afetados e dos próprios agentes estatais. No âmbito da segurança pública, observou-se que essa condição compromete a legitimidade das decisões mediadas por tecnologias inteligentes, uma vez que obstaculiza a identificação dos critérios que fundamentam correlações biométricas. Sob esse prisma, verificou-se que a opacidade cerceia o exercício da ampla defesa e fragiliza o controle democrático.

Em seguida, o trabalho tratou da responsabilidade pelas decisões produzidas com auxílio de sistemas algorítmicos. A investigação demonstrou que a atribuição de responsabilidade deve recair sobre os agentes humanos e institucionais envolvidos na concepção, aquisição, implementação, fiscalização e utilização dessas ferramentas. Isso porque a inteligência artificial foi caracterizada como um instrumento destituído de consciência, intencionalidade ou personalidade jurídica própria. Essa análise possibilitou o afastamento da transferência simbólica de responsabilidade ao aparato tecnológico e corroborou a imprescindibilidade do controle jurídico sobre programadores, fornecedores, administradores públicos, órgãos de segurança e outras autoridades que se valem dos resultados automatizados.

No terceiro capítulo, a investigação analisou o funcionamento das tecnologias de

identificação facial. O estudo descreveu as fases de detecção da face, extração de características biométricas, elaboração de mapas faciais, comparação com bases de dados e geração de resultados baseados em cálculos de probabilidade. Foram examinadas, adicionalmente, as variáveis que interferem na confiabilidade dos sistemas, tais como a qualidade da imagem e a iluminação. Essa exposição permitiu compreender que o reconhecimento facial é condicionado por um conjunto de escolhas técnicas e institucionais que influenciam diretamente os seus resultados, os quais, por vezes, encontram-se vinculados a valores e interesses humanos.

Posteriormente, a investigação territorializou a discussão no estado do Ceará. A pesquisa examinou a evolução do monitoramento no Brasil e no Ceará, desde os investimentos associados a megaeventos esportivos até a consolidação de uma infraestrutura tecnológica voltada à segurança pública. No âmbito cearense, analisaram-se a proliferação de câmeras de videomonitoramento, o emprego de sistemas inteligentes na segurança pública e a unificação dos fluxos de dados governamentais. O estudo também escrutinou a função dos discursos institucionais na legitimação dessas ferramentas. A análise evidenciou que a expansão tecnológica ocorreu em um cenário de carência de parâmetros normativos uniformes e de restrição ao acesso a informações públicas.

Na seção seguinte, a pesquisa estabeleceu o nexo entre o reconhecimento facial e a seletividade racial do sistema punitivo cearense. A teoria do etiquetamento e o conceito de sujeição criminal foram empregados para a compreensão da construção social da criminalidade e da formação de identidades desviantes. A análise demonstrou que determinados sujeitos e territórios são historicamente vinculados às ideias de perigo, desordem e criminalidade, notadamente em sociedades estruturadas por desigualdades raciais. A exposição de indicadores relativos ao encarceramento e à letalidade contra a população negra permitiu situar o cenário cearense em uma dinâmica mais abrangente de criminalização da negritude. Nesse contexto, verificou-se que os sistemas de reconhecimento facial tendem a automatizar estratificações sociais quando utilizam bases de dados enviesadas e quando são aplicados em práticas policiais orientadas por padrões seletivos de suspeição.

Por fim, o trabalho examinou os limites jurídicos da aplicação de tecnologias biométricas pelo Estado, com especial atenção à Lei Geral de Proteção de Dados Pessoais. A pesquisa demonstrou que a exclusão das atividades de segurança pública e persecução penal do campo principal de incidência da LGPD cria uma relevante lacuna normativa. Essa circunstância amplia a margem de atuação estatal em matéria de vigilância e controle social,

dificultando a instituição de mecanismos de transparência, auditabilidade e responsabilização. A análise das propostas de regulamentação, incluindo os debates em torno da “LGPD Penal”, indicou a necessidade de um arcabouço específico para disciplinar o uso de tecnologias biométricas em atividades de natureza securitária.

Esse percurso analítico também permitiu reconhecer as limitações da presente pesquisa. A investigação concentrou-se no Ceará e foi desenvolvida com base em documentos públicos, o que restringiu o acesso a elementos técnicos mais detalhados sobre os sistemas eventualmente empregados na segurança pública do estado, tais como códigos-fonte, bases de dados, contratos administrativos, protocolos internos e métricas técnicas. Esse obstáculo, todavia, confirma a própria relevância do problema examinado, na medida em que a dificuldade de acesso a informações integra o campo de opacidade que envolve a implementação dessas tecnologias.

Além disso, a pesquisa analisou riscos sociotécnicos e jurídicos, sem pretender mensurar impactos causais definitivos ou estabelecer comparação estatística entre períodos anteriores e posteriores à adoção dos sistemas biométricos, sobretudo pela insuficiência de dados públicos sistematizados. Para investigações futuras, revela-se imprescindível o aprofundamento de estudos empíricos sobre o funcionamento concreto dessas tecnologias no Ceará e em outros estados brasileiros, com análise de contratos públicos, auditorias independentes, protocolos de abordagem e outros mecanismos de controle externo. É igualmente necessária a realização de pesquisas interdisciplinares, a fim de avaliar como a vigilância biométrica incide sobre grupos vulnerabilizados e quais parâmetros normativos podem assegurar transparência, responsabilização, contestabilidade e proteção efetiva dos direitos fundamentais.

Diante desse panorama, conclui-se que as tecnologias de reconhecimento facial aplicadas à segurança pública do Ceará podem contribuir para a perpetuação de práticas discriminatórias quando inseridas em um ecossistema caracterizado pela seletividade do aparato penal, pela opacidade algorítmica, pela assimetria racial e pela fragilidade normativa. Ao longo deste estudo, observou-se que a proteção de dados pessoais, a igualdade racial, o devido processo legal e os direitos fundamentais devem compor uma mesma agenda regulatória. Em um Estado Democrático de Direito, a tecnologia biométrica deve, portanto, permanecer subordinada à preservação das garantias constitucionais.

REFERÊNCIAS

- AGUIAR, Guilherme Nobre. **Teoria do etiquetamento social, criminalização e estigmatização de jovens periféricos**. 2021. Dissertação (Mestrado em Desenvolvimento Social) – Universidade Estadual de Montes Claros, Minas Gerais, 2021. Disponível em: <https://repositorio.unimontes.br/handle/1/1401>. Acesso em: 2 abr. 2026.
- ALEX, Robert. **Teoria dos direitos fundamentais**. São Paulo: Malheiros, 2008.
- ALMEIDA, Silvio Luiz de. **Racismo estrutural**. São Paulo: Sueli Carneiro; Pólen, 2019.
- AZEVEDO, Cynthia Picolo Gonzaga de; LIMA, Eliz Marina Bariviera de; SILVA, Felipe Rocha da; RODRIGUES, Gustavo Ramos; DUTRA, Luiza Corrêa de Magalhães; SANTARÉM, Paulo Rená da Silva; RODRIGUES, Victor Barbieri Vieira Rodrigues. **Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022**. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), p. 1-29, 2022. Disponível em: <https://lapin.org.br/wp-content/uploads/2022/11/Nota-tecnica-Analise-comparativa-entre-o-anteprojeto-de-LGPD-Penal-e-o-PL-15152022-1.pdf>. Acesso em: 9 abr. 2026.
- BADARÓ, Gustavo. **A cadeia de custódia da prova digital**. Direito probatório. Londrina: Thoth, 2023.
- BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim IBCCRIM**, São Paulo, v. 29, n. 343, p. 7-9, 2024. Disponível em: https://www.publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1325. Acesso em: 30 abr. 2026.
- BARASSI, Veronica. Datafied times: Surveillance capitalism, data technologies and the social construction of time in family life. **New Media & Society**, v. 22, n. 9, p. 1545-1560, 2020. Disponível em: <https://doi.org/10.1177/1461444820913573>. Acesso em: 22 out. 2025.
- BARRETO, Helena do Rêgo; FERREIRA, Katiele Gomes. Solucionismo Tecnológico e Segurança Pública no Ceará: análise discursiva da campanha da Nova Estratégia de Segurança Pública (NESP). In: Congresso Brasileiro de Ciências da Comunicação, 46., 2023, São Paulo. **Anais [...]** São Paulo: Intercom, 2023. p. 1-15. Disponível em: https://sistemas.intercom.org.br/pdf/link_aceite/nacional/11/0816202323071264dd80d004f0c.pdf. Acesso em: 5 abr. 2026.
- BARROS, João Paulo Pereira; PAIVA, Luiz Fábio Silva; RODRIGUES, Jéssica Silva; SILVA, Dagualberto Barboza da; LEONARDO, Camila dos Santos. Pacificação nas periferias: discursos sobre as violências e o cotidiano de juventudes em Fortaleza. **Revista de Psicologia**, Fortaleza, v. 9, n. 1, p. 117-128, 2018. Disponível em: <http://repositorio.ufc.br/handle/riufc/32862>. Acesso em: 2 abr. 2026.
- BAUMAN, Zygmunt. **Medo líquido**. Rio de Janeiro: Zahar, 2008.
- BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**. Rio de Janeiro: Zahar, 2014.

BECHARA, Ana Elisa Liberatore Silva. Discursos de emergência e política criminal: o futuro do direito penal brasileiro. **Revista da Faculdade de Direito**, São Paulo, v. 103, p. 411-436, 2008. Disponível em: <https://revistas.usp.br/rfdusp/article/view/67812>. Acesso em: 23 set. 2025.

BECK, Ulrich. **Risk society**. Towards a new modernity. Londres: Sage Publications, 1992.

BECKER, Howard S. **Outsiders**: estudos de sociologia do desvio. Rio de Janeiro: Zahar, 2008.

BEER, David. The social power of algorithms. **Information Communication and Society**, [S. l.], v. 20, n. 1, p. 1-13, 2017. Disponível em: <https://doi.org/10.1080/1369118X.2016.1216147>. Acesso em: 4 jan. 2026.

BENICIO, Luis Fernando de Souza; BARROS, João Paulo Pereira; RODRIGUES, Jéssica Silva; SILVA, Dagualberto Barboza da; LEONARDO, Camila dos Santos; COSTA, Aldemar Ferreira da. Necropolítica e Pesquisa-Intervenção sobre Homicídios de Adolescentes e Jovens em Fortaleza, CE. **Psicologia: ciência e profissão**, Brasília, v. 38, p. 192-207, 2018. Disponível em: <https://doi.org/10.1590/1982-3703000212908>. Acesso em: 2 abr. 2026.

BENJAMIN, Ruha. **Race After Technology**: Abolitionist Tools for the New Jim Code. Cambridge: Polity Press, 2019.

BENTO, Cida. **O pacto da branquitude**. São Paulo: Companhia das Letras, 2022.

BEZERRA, Arthur Coelho; COSTA, Camila Mattos da. Pele negra, algoritmos brancos: informação e racismo nas redes sociotécnicas. **Liinc em Revista**, v. 18, n. 2, p. 1-14, 2022. Disponível em: <https://doi.org/10.18617/liinc.v18i2.6043>. Acesso em: 23 ago. 2025.

BIONI, Bruno R.; MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. p. 791-813.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: A Função e os Limites do Consentimento. São Paulo: Revista dos Tribunais, 2020.

BIONI, Bruno Ricardo; LUCIANO, Maria. O princípio da precaução na regulação da inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada? In: FRAZÃO, Ana; MOULHOLLAND, Caitlin (coord.). **Inteligência artificial e direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters, 2019. p. 208-231.

BOEING, Daniel Henrique Arruda; ROSA, Alexandre Moraes da. **Ensinando um robô a julgar**: pragmática, discricionariedade, heurísticas e vieses no uso de aprendizado de máquina no judiciário. Florianópolis: Emais Academia, 2020.

BOWEN, Sthefanie M. Man vs. Machine: Facial Recognition Technology Replacing Eyewitness Identifications. **Lincoln Memorial University Law Review**, v. 10, n. 1, p. 21-69, 2022. Disponível em: <https://digitalcommons.lmunet.edu/cgi/viewcontent.cgi?article=1178&context=lmulrev>. Acesso em: 7 abr. 2026.

BOYD, Danah; CRAWFORD, Kate. Critical questions for big data. Provocations for a cultural, technological, and scholarly phenomenon. **Information, Communication & Society**, v. 15, n. 5, p. 662-679, 2012. Disponível em: <https://doi.org/10.1080/1369118X.2012.678878>. Acesso em: 17 out. 2025.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 1.515, de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília, DF: Câmara dos Deputados, 2022b. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300#tramitacoes>. Acesso em: 9 abr. 2026.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 6 abr. 2026.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Diário Oficial da União: seção 1, Brasília, DF, n. 30, p. 2, 10 fev. 2022. Disponível em: <https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=11/02/2022&jornal=515&pagina=2&totalArquivos=269>. Acesso em: 11 abr. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Diário Oficial da União, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 12 abr. 2026.

BRASIL. Ministério da Justiça e Segurança Pública. **Portaria nº 793, de 24 de outubro de 2019**. Diário Oficial da União: seção 1, Brasília, DF, edição 208, p. 55, 24 out. 2019. Disponível em: <https://in.gov.br/en/web/dou/-/portaria-n-793-de-24-de-outubro-de-2019-223853575>. Acesso em: 20 nov. 2025.

BRASIL. Ministério da Justiça e Segurança Pública. **Portaria nº 961, de 24 de junho de 2025**. Diário Oficial da União: seção 1, Brasília, DF, edição 120, p. 104, 30 jun. 2025. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-mj-sp-n-961-de-24-de-junho-de-2025-638661609>. Acesso em: 8 maio 2026.

BRASIL. Superior Tribunal de Justiça. **Habeas Corpus n. 1.059.475**. Paciente: Fabio Ferreira Dias Marcondes. Impetrante: Edlenio Xavier Barreto. Relator: Min. Reynaldo Soares da Fonseca. Brasília, DF, 10 abr. 2026. Disponível em: https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=5&documento_sequencial=368872710®istro_numero=202504872020&peticao_numero=&publicacao_data=20260414&formato=PDF. Acesso em: 30 abr. 2026.

BRAYNE, Sarah. **Predict and surveil**: data, discretion, and the future of policing. New York: Oxford University Press, 2021.

BRAYNE, Sarah. The Banality of Surveillance. **Surveillance & Society**, v. 20, n. 4, p. 372-378, 2022. Disponível em: <https://doi.org/10.24908/ss.v20i4.15946>. Acesso em: 13 out. 2025.

BRICEÑO-LEON, Roberto; BARREIRA, César; AQUINO, Jania Perla Diógenes de. Facções de Fortaleza y colectivos de Caracas: dos modelos de gobernanza criminal. **Dilemas**: Revista de Estudos de Conflito e Controle Social, Rio de Janeiro, v. 15, n. 4, p. 21-49, 2022. Disponível em: <http://dx.doi.org/10.4322/dilemas.v15nsp4.46522>. Acesso em: 4 jan. 2026.

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

BUCAR, Daniel; VIOLA, Mario. Tratamento de dados pessoais por “legítimo interesse do controlador”: primeiras questões e apontamentos. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. p. 459-478.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: Intersectional accuracy disparities in commercial gender classification. **Proceedings of Machine Learning Research**, p. 1-15, 2018. Disponível em: proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Acesso em: 12 jan. 2026.

BURDEAU, Georges. **Méthode de la science politique**. Paris: Dalloz, 1959.

BURDON, Mark; COHEN, Tegan. Modulation Harms and the Google Home. **Surveillance & Society**, v. 19, n. 2, p. 154-167, 2021. Disponível em: <https://doi.org/10.24908/ss.v19i2.14299>. Acesso em: 13 out. 2025.

BURRELL, Jenna. How the machine ‘thinks’: Understanding opacity in machine learning algorithms. **Big Data & Society**, v. 3, n. 1, p. 1-12, 2016. Disponível em: <https://doi.org/10.1177/2053951715622512>. Acesso em: 7 jan. 2026.

CAMPELLO, Ricardo Urquizas. **Curto-circuito**: monitoramento eletrônico e tecnopunição no Brasil. Lisboa: Etnográfica Press, 2021.

CANHADAS, Fernando Augusto Martins. A Lei de Acesso à Informação e a Lei Geral de Proteção de Dados: a transparência proibida. *In*: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes. **LGPD e Administração Pública**: uma análise ampla dos impactos. São Paulo: Revista dos Tribunais, 2020. p. 245-444.

CAPOVILLA, Cristiano Lenardo. As sociedades de controle: forma hegemônica da acumulação capitalista e padrão de poder da gestão institucional em Gilles Deleuze. **Revista Interdisciplinar em Cultura e Sociedade**, São Luís, v. 5, n. 2, p. 262-275, 2019. Disponível em: <https://periodicoseletronicos.ufma.br/index.php/ricultsociedade/article/view/13016>. Acesso em: 30 ago. 2025.

CARDOSO, Bruno. Estado, tecnologias de segurança e normatividade neoliberal. *In*: BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; GUILHON, Luciana; MELGAÇO, Lucas (org.). **Tecnopolíticas da vigilância**: perspectivas da margem. São Paulo: Boitempo, 2018. p. 91-105.

CARNEIRO, Sueli. **Dispositivo de racialidade**: a construção do outro como não-ser como fundamento do ser. Rio de Janeiro: Zahar, 2023.

CASTELLS, Manuel. **A sociedade em rede**. A era da informação: economia, sociedade e cultura. 6. ed. São Paulo: Paz e Terra, 1999. v. 1.

CASTELLS, Manuel. Internet e sociedade em rede. *In*: MORAES, Dênis de (org.). **Por uma outra comunicação** - mídia, mundialização cultural e poder. Rio de Janeiro: Record, 2003. p. 255-287.

CASTRO, Lucas. **Com uso do reconhecimento facial do Governo do Ceará, homem com mandado de prisão em aberto é preso em estádio durante clássico-rei**. Secretaria da Segurança Pública e Defesa Social do Ceará (SSPDS-CE), Fortaleza, 2025. Disponível em: <https://www.sspds.ce.gov.br/2025/03/15/com-uso-do-reconhecimento-facial-do-governo-do-ceara-homem-com-mandado-de-prisao-em-aberto-e-presos-em-estadio-durante-classico-rei/>. Acesso em: 5 abr. 2026.

CATH, Corinne; WATCHER, Sandra; MITTELSTADT, Brent; TADDEO, Mariarosaria; FLORIDI, Luciano. Artificial Intelligence and the ‘Good Society’: the US, EU, and UK approach. **Science and Engineering Ethics**, v. 24, p. 505-528, 2018. Disponível em: <https://doi.org/10.1007/s11948-017-9901-7>. Acesso em: 14 jan. 2026.

CEARÁ. Fundação Cearense de Apoio ao Desenvolvimento Científico e Tecnológico (Funcap). **Plataforma multibiométrica e monitoramento inteligente**. Fortaleza, [s.d.]. Disponível em: <https://vitrinefuncap.com/projeto/11270/detalhes>. Acesso em: 10 abr. 2026.

CEARÁ. Governo do Estado do Ceará. **Big Data da Segurança Pública, Spia e videomonitoramento da SSPDS são utilizados na elucidação de crime em Fortaleza**. Fortaleza: Governo do Estado do Ceará, 13 de dezembro de 2019. Disponível em: <https://www.ce.gov.br/2019/12/13/big-data-da-seguranca-publica-spia-e-videomonitoramento-da-sspds-sao-utilizados-na-elucidacao-de-crime-em-fortaleza/>. Acesso em: 3 abr. 2026.

CEARÁ. Governo do Estado do Ceará. **FORTaleCE: Centro Integrado de Videomonitoramento de Fortaleza reúne mais de 7 mil câmeras e tem integração com Ciops**. Fortaleza: Governo do Estado do Ceará, 7 de abril de 2026. Disponível em: <https://www.ce.gov.br/2026/04/07/fortalece-centro-integrado-de-videomonitoramento-de-fortaleza-reune-mais-de-7-mil-cameras-e-tem-integracao-com-ciops/>. Acesso em: 10 abr. 2026.

CEARÁ. Governo do Estado do Ceará. Secretaria da Segurança Pública e Defesa Social do Ceará (SSPDS-CE). **Com uso do reconhecimento facial, homem com mandado de prisão em aberto é preso em Maracanaú**. Fortaleza, 22 de junho de 2025. 2025a. Disponível em: <https://www.sspds.ce.gov.br/2025/06/22/com-uso-do-reconhecimento-facial-homem-com-mandado-de-prisao-em-aberto-e-presos-em-maracanau/>. Acesso em: 5 abr. 2026.

CEARÁ. Governo do Estado do Ceará. Secretaria da Segurança Pública e Defesa Social do Ceará (SSPDS-CE). **Foragido da Justiça é capturado pela PCCE com o auxílio de reconhecimento facial**. Fortaleza, 10 de fevereiro de 2020. 2020b. Disponível em: <https://www.sspds.ce.gov.br/2020/02/10/foragido-da-justica-e-capturado-pela-pcce-com-o-auxilio-de-reconhecimento-facial-desenvolvido-pela-sspds/>. Acesso em: 5 abr. 2026.

CEARÁ. Governo do Estado do Ceará. Secretaria da Segurança Pública e Defesa Social do Ceará (SSPDS-CE). **Polícia Civil do CE prende paulista foragido da Justiça do DF com**

reconhecimento facial. Fortaleza, 12 de agosto de 2020. 2020d. Disponível em: <https://www.sspds.ce.gov.br/2020/08/12/policia-civil-do-ce-prende-paulista-foragido-da-justica-do-df-com-auxilio-do-reconhecimento-facial-da-sspds/>. Acesso em: 5 abr. 2026.

CEARÁ. Governo do Estado do Ceará. Secretaria da Segurança Pública e Defesa Social do Ceará (SSPDS-CE). **Suspeito de roubar farmácia é preso pela Polícia Civil com auxílio do reconhecimento facial.** Fortaleza, 29 de abril de 2020. 2020a. Disponível em: <https://www.sspds.ce.gov.br/2020/04/29/suspeito-de-roubar-farmacia-e-presos-pela-policia-civil-com-auxilio-do-reconhecimento-facial/>. Acesso em: 5 abr. 2026.

CEARÁ. Governo do Estado do Ceará. Secretaria da Segurança Pública e Defesa Social do Ceará (SSPDS-CE). **Suspeito de roubo é preso com o auxílio do reconhecimento facial da SSPDS.** Fortaleza, 29 de outubro de 2020. 2020c. Disponível em: <https://www.sspds.ce.gov.br/2020/10/29/suspeito-de-roubo-e-presos-com-o-auxilio-do-reconhecimento-facial-da-sspds/>. Acesso em: 5 abr. 2026.

CEARÁ. Governo do Estado do Ceará. **Sistema de Reconhecimento Facial é implementado em todos os setores da Arena Castelão, com mais de 123 mil cadastros realizados com sucesso.** Fortaleza: Governo do Estado do Ceará, 31 de março de 2025. 2025b. Disponível em: <https://www.ce.gov.br/2025/03/31/sistema-de-reconhecimento-facial-e-implementado-em-todos-os-setores-da-arena-castelao-com-mais-de-123-mil-cadastros-realizados-com-sucesso/>. Acesso em: 3 abr. 2026.

CEARÁ. Governo do Estado do Ceará. **SSPDS lança ferramenta Status para identificação de manchas criminais e tomadas de decisão.** Fortaleza: Governo do Estado do Ceará, 4 de fevereiro de 2021. 2021b. Disponível em: <https://www.ce.gov.br/2021/02/04/sspds-lanca-ferramenta-status-para-identificacao-de-manchas-criminais-e-tomadas-de-decisao/>. Acesso em: 3 abr. 2026.

CEARÁ. Governo do Estado do Ceará. **Supesp e Cientista-chefe: ciência a serviço da segurança pública no Ceará.** Fortaleza: Governo do Estado do Ceará, 2023. Disponível em: <https://www.ce.gov.br/2023/10/26/supesp-e-cientista-chefe-ciencia-a-servico-da-seguranca-publica-no-ceara/>. Acesso em: 3 abr. 2026.

CEARÁ. **Lei nº 17.378, de 4 de janeiro de 2021.** Institui, no âmbito do estado do Ceará, o programa Cientista-Chefe. Fortaleza: Diário Oficial do Estado, 4 de janeiro de 2021. 2021a. Disponível em: <https://www.funcap.ce.gov.br/wp-content/uploads/sites/52/2021/05/LEI-ESTADUAL-17378-2020-PROGRAMA-CIENTISTA-CHEFE.pdf>. Acesso em: 12 abr. 2026.

CEARÁ. Secretaria da Segurança Pública e Defesa Social do Ceará (SSPDS-CE). Superintendência de Pesquisa e Estratégia de Segurança Pública (Supesp-CE). **Tecnologias.** Fortaleza: Supesp-CE, [s.d.]. Disponível em: https://www.supesp.ce.gov.br/wp-content/uploads/sites/89/2022/11/TECNOLOGIAS_GERAL.pdf. Acesso em: 3 abr. 2026.

CEARÁ. Tribunal de Justiça do Estado do Ceará. **Habeas Corpus Criminal n. 0623986-18.2025.8.06.0000.** Paciente: Felipe Andrade de Oliveira. Impetrantes: Felipe Folchini Machado e Bruno Leonardo Ledesma Risso. Relatora: Des. Sílvia Soares de Sá Nóbrega. Fortaleza, CE, 27 de maio de 2025. 2025c. Disponível em: <https://esaj.tjce.jus.br/cjsj/getArquivo.do?cdAcordao=3798636&cdForo=0>. Acesso em: 7 jun. 2026.

CEARÁ. Tribunal de Justiça do Estado do Ceará. **Habeas Corpus Criminal n. 0625260-17.2025.8.06.0000**. Paciente: José Hildebrandes Ferreira. Impetrante: Larissa Pereira Soares. Relatora: Des. Andréa Mendes Bezerra Delfino. Fortaleza, CE, 8 de julho de 2025. 2025d. Disponível em: <https://esaj.tjce.jus.br/cjsg/getArquivo.do?cdAcordao=3805503&cdForo=0>. Acesso em: 7 jun. 2026.

CERQUEIRA, Daniel; BUENO, Samira (coord.). **Atlas da violência 2025**. Brasília: Ipea; FBSP, 2025. Disponível em: <https://www.ipea.gov.br/atlasviolencia/arquivos/artigos/5999-atlasdaviolencia2025.pdf>. Acesso em: 14 jan. 2025.

CHAVES, Oriana. Apontamentos sobre a inteligência artificial no programa Cientista-Chefe do Ceará. In: PARANÁ, Edemilson; SANTAELLA, Rodrigo (org.). **Estado e inteligência artificial: o caminho brasileiro e os usos cearenses**. Fortaleza: EdUECE, 2025. p. 53-77. Disponível em: <https://www.uece.br/eduece/wp-content/uploads/sites/88/2025/10/Estado-e-Intelig%C3%Aancia-Artificial-o-caminho-brasileiro-e-os-usos-cearenses.pdf>. Acesso em: 4 maio 2026.

COLE, Simon. **Suspect Identities: A History of Fingerprinting and Criminal Identification**. Cambridge: Harvard University Press, 2001.

COMITÊ CEARENSE PELA PREVENÇÃO DE HOMICÍDIOS NA ADOLESCÊNCIA. **Cada Vida Importa**. Relatório Final. Fortaleza: Governo do Estado do Ceará; Assembleia Legislativa do Estado do Ceará, Comitê Cearense pela Prevenção de Homicídios na Adolescência, Instituto OCA, 2016. Disponível em: <https://cadavidaimporta.com.br/wp-content/uploads/2023/05/cada-vida-importa-relatorio-final.pdf>. Acesso em: 2 abr. 2026.

COMITÊ PARA ELIMINAÇÃO DA DISCRIMINAÇÃO RACIAL. **Recomendação Geral nº 36, de 24 de novembro de 2020**. Prevenção e combate ao perfilamento racial por agentes policiais. [S. l.], 2020. Disponível em: https://acnudh.org/wp-content/uploads/2020/12/CERD_C_GC_36_PORT_REV.pdf. Acesso em: 15 abr. 2026.

CONSELHO NACIONAL DE JUSTIÇA. **Grupo de trabalho: reconhecimento de pessoas**. Brasília: CNJ, 2022. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2023/05/relatorio-gt-reconhecimento-de-pessoas-v5-17-10-2022.pdf>. Acesso em: 2 abr. 2026.

CORRÊA, Bianca Kremer Nogueira. **Direito e tecnologia em perspectiva amefricana: autonomia, algoritmos e vieses raciais**. 2021. Tese (Doutorado em Direito) – Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2021. Disponível em: <https://www.maxwell.vrac.puc-rio.br/58993/58993.PDF>. Acesso em: 15 mar. 2026.

COSTA, Carlos Zoete Gomes da; ABREU, Daniel Quintaneiro. O uso de inteligência artificial na análise de documentos forenses: uma revisão sistemática. **Revista Base Científica**, Piauí, v. 2, p. 1-20, 2024. Disponível em: <https://bio10publicacao.com.br/base/article/view/503>. Acesso em: 30 abr. 2026.

CRAWFORD, Neta C. Institutionalizing passion in world politics: fear and empathy. **International Theory**, v. 6, n. 3, p. 535-557, 2014. Disponível em: 10.1017/S1752971914000256. Acesso em: 20 out. 2025.

CRESTANE, Dérique Soares; LEAL, Mônica Clarissa Hennig. **Discriminação algorítmica e discriminação estrutural** [livro eletrônico]: standards protetivos da corte interamericana de direitos humanos e do Supremo Tribunal Federal. São Paulo: Tirant lo Blanch, 2024.

CRUZ, Rogerio Schietti. Investigação criminal, reconhecimento de pessoas e erros judiciais: considerações em torno da nova jurisprudência do Superior Tribunal de Justiça. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 8, n. 2, p. 567-600, 2022. Disponível em: <https://revista.ibraspp.com.br/RBDPP/article/view/717>. Acesso em: 24 abr. 2026.

DELEUZE, Gilles. **Conversações, 1972-1990**. Tradução de Peter Pál Pelbart. São Paulo: Ed. 34, 1992.

DESCARTES, René. **Discurso do Método**. Tradução de Paulo Neves. Porto Alegre: L&PM, 2005.

DIETER, Maurício. **Política criminal atuarial: a criminologia do fim da história**. 2012. Tese (Doutorado em Direito) – Universidade Federal do Paraná, Curitiba, 2012. Disponível em: <https://acervodigital.ufpr.br/xmlui/bitstream/handle/1884/28416/R%20-%20T%20-%20MAURICIO%20STEGEMANN%20DIETER.pdf?sequence=1&isAllowed=y>. Acesso em: 4 abr. 2026.

DIGNAM, Alan. Artificial intelligence, tech corporate governance and the public interest regulatory response. **Cambridge Journal of Regions, Economy and Society**, v. 13, n. 1, p. 37-54, 2020. Disponível em: <https://doi.org/10.1093/cjres/rsaa002>. Acesso em: 8 jan. 2026.

DOMINGOS, Pedro. **A revolução do algoritmo mestre: como a aprendizagem automática está a mudar o mundo**. Lisboa: Editora Manuscrito, 2017a.

DOMINGOS, Pedro. **O Algoritmo Mestre: como a busca pelo algoritmo de machine learning definitivo recriará nosso mundo**. São Paulo: Novatec Editora, 2017b.

DONEDA, Danilo; MENDES, Laura. Reflexões iniciais sobre a nova lei geral de proteção de dados. **Revista de Direito do Consumidor**. São Paulo, v. 27, n. 120, 2018. p. 469-483.

DUARTE, Daniel Edler. Tecnopolíticas da falha: dispositivos de crítica e resistência a novas ferramentas punitivas. **Revista Brasileira de Ciências Sociais**, São Paulo, v. 39, p. 1-18. Disponível em: <https://doi.org/10.1590/39017/2024>. Acesso em: 3 abr. 2026.

DUARTE, Daniel Edler; NUNES, Pablo; LIMA, Thallita G. L. **Estudos de vigilância** [livro eletrônico]. Coleção Panorama. 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: 4 maio 2026.

DUARTE, Evandro Piza; CARVALHO NETTO, Menelick de. A Cidade da Guerra e a Repressão Humanitária: as Fantasias de Katsuhiko Otomo sobre a Cidade Fortaleza. In: ZACKESKI, Cristina; DUARTE, Evandro C. Piza (org.). **Criminologia e cinema: perspectivas sobre o controle social**. Brasília: UniCEUB, 2012. p. 67-129.

EUBANKS, Virginia. **Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor**. New York: St. Martin's Press, 2018.

FALCÃO, Larissa. **Ceará contra o Crime**: Estado vai realizar novos concursos e implementar reconhecimento facial e rastreamento de motos. Secretaria da Segurança Pública e Defesa Social do Ceará (SSPDS-CE), Fortaleza, 2024. Disponível em: <https://www.sspds.ce.gov.br/2024/08/26/ceara-contra-o-crime-estado-vai-realizar-novos-concursos-e-implementar-reconhecimento-facial-e-rastreamento-de-motos/>. Acesso em: 5 abr. 2026.

FANON, Frantz. **Pele negra, máscaras brancas**. Tradução de Renato da Silveira. Salvador: EDUFBA, 2008.

FEENBERG, Andrew. **Entre a Razão e a Experiência**: ensaios sobre tecnologia e modernidade. Tradução de Eduardo Beira, Cristiano Cruz e Ricardo Neder. Portugal: Inovatec - MTI Portugal, 2017.

FEENBERG, Andrew. Racionalização Subversiva: tecnologia, poder e democracia. *In*: NEDER, Ricardo T. (org.). **A teoria crítica de Andrew Feenberg**: racionalização democrática, poder e tecnologia. 2. ed. Brasília: OBMTS, 2013. p. 67-95.

FELDMAN, Shelley. Social Regulation in the Time of War: Constituting the Current Crisis. **Globalizations**, New York, v. 4, n. 4, p. 445-459, 2007. Disponível em: <https://doi.org/10.1080/14747730701695646>. Acesso em: 22 set. 2025.

FELDMAN, Shelley. Surveillance and Securitization. *In*: FELDMAN, Shelley; GEISLER, Charles; MENON, Gayatri A. (ed.). **Accumulating insecurity**: violence and dispossession in the making of everyday life. Athens: University of Georgia Press, 2011. p. 185-212.

FELTRAN, Gabriel; LERO, Cecilia; CIPRIANI, Marcelli; MALDONADO, Janaina; RODRIGUES, Fernando de Jesus; SILVA, Luiz Eduardo Lopes; FARIAS, Nido. Variações nas taxas de homicídios no Brasil: Uma explicação centrada nos conflitos faccionais. **Dilemas**: Revista de Estudos de Conflito e Controle Social, Rio de Janeiro, v. 15, p. 311-348, 2022. Disponível em: <https://doi.org/10.4322/dilemas.v15nsp4.46920>. Acesso em: 8 abr. 2026.

FENOLL, Jordi Nieva. **Inteligencia artificial y proceso judicial**. Madrid, Barcelona, Buenos Aires, São Paulo: Marcial Pons, 2018.

FERNANDES, Fernando Andrade; RESENDE, Ana Paula Bougleux Andrade. Regulamentação do tratamento automatizado de dados pessoais em matéria penal. **Suprema**: Revista de Estudos Constitucionais, Distrito Federal, Brasil, v. 3, n. 1, p. 471-500, 2023. Disponível em: <https://suprema.stf.jus.br/index.php/suprema/article/view/207>. Acesso em: 4 abr. 2026.

FERREIRA, Felipe Fernando Abreu. **As novas leis da robótica de Frank Pasquale frente à opacidade da inteligência artificial**. 2024. Dissertação (Mestrado em Direito) – Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2024. Disponível em: <https://www.bdtd.uerj.br:8443/bitstream/1/22423/2/Disserta%3%a7%3%a3o%20-%20Felipe%20Fernando%20Abreu%20Ferreira%20-%202024%20-%20Completa.pdf>. Acesso em: 15 mar. 2026.

FERRER-BELTRÁN, Jordi. **Prova sem convicção**: standards de prova e devido processo. Tradução de Vitor de Paula Ramos. Salvador: Editora Juspodivm, 2022.

FIRMINO, Rodrigo José. Securitização, vigilância e territorialização em espaços públicos. *In*: BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; GUILHON, Luciana; MELGAÇO, Lucas (org.). **Tecnopolíticas da vigilância**: perspectivas da margem. São Paulo: Boitempo, 2018. p. 69-89.

FLAUZINA, Ana Luiza Pinheiro. **Corpo negro caído no chão**: o sistema penal e o projeto genocida do Estado brasileiro. 2006. Dissertação (Mestrado em Direito) – Universidade de Brasília, Brasília, 2006. Disponível em: <http://repositorio.unb.br/handle/10482/5117>. Acesso em: 5 abr. 2026.

FLICK, Uwe. **Introdução à pesquisa qualitativa**. 3. ed. Porto Alegre: ArtMed, 2008. *E-book*. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9788536318523/>. Acesso em: 14 maio 2025.

FLORIDI, Luciano. **The 4th Revolution**: How the Infosphere Is Reshaping Human Reality. UK: Oxford University Press, 2014.

FORTALEZA. Prefeitura Municipal. **Prefeitura e Governo inauguram Centro Integrado de Videomonitoramento, com acesso a mais de 7 mil câmeras**. Fortaleza, 2026. Disponível em: <https://www.fortaleza.ce.gov.br/noticias/prefeitura-e-governo-inauguram-centro-integrado-de-videomonitoramento-com-acesso-a-mais-de-7-mil-cameras>. Acesso em: 10 abr. 2026.

FOTO de astro do cinema Michael B. Jordan aparece em lista de procurados pela polícia do Ceará. **G1**, Ceará, 7 jan. 2022. Disponível em: <https://g1.globo.com/ce/ceara/noticia/2022/01/07/astro-do-cinema-michael-b-jordan-aparece-em-lista-de-procurados-pela-policia-do-ceara.ghtml>. Acesso em: 6 abr. 2026.

FOUCAULT, Michel. **Em Defesa da Sociedade**. São Paulo: Martins Fontes, 1999.

FOUCAULT, Michel. Governmentality. Tradução de Rosi Braidotti. *In*: BURCHELL, Graham; GORDON, Colin; MILLER, Peter (ed.). **The Foucault Effect**: Studies in Governmentality. Chicago: University of Chicago Press, 1991. p. 87-104.

FOUCAULT, Michel. **História da sexualidade I**: A vontade de saber. 16. ed. Rio de Janeiro: Edições Graal, 2005.

FOUCAULT, Michel. **Segurança, Território, População**. Curso dado no Collège de France (1977-1978). São Paulo: Martins Fontes, 2008.

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. Petrópolis: Editora Vozes, 2001.

FRAZÃO, Ana. **Dever geral de cuidado das plataformas diante de crianças e adolescentes**. Parecer Jurídico. São Paulo: Instituto Alana, 2021. Disponível em: <https://criancaeconsumo.org.br/wp-content/uploads/2021/11/dever-geral-de-cuidado-das-plataformas.pdf>. Acesso em: 5 maio 2026.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. p. 23-52.

FRAZÃO, Ana. Inteligência Artificial e seus desafios no Direito Penal. In: MENDES, Gilmar Ferreira; FREITAS, Matheus Pimenta de (coord.). **Constituição, Direito Penal e Novas Tecnologias**. São Paulo: Almedina, 2023. p. 23-45.

FRAZÃO, Ana. Plataformas digitais, big data e riscos para os direitos da personalidade. In: TEPEDINO, Gustavo; MENEZES, Joyceane (coord.). **Autonomia privada, liberdade existencial e direitos fundamentais**. Belo Horizonte: Fórum, 2019. p. 333-349.

FREIRE, Ana Alice; BARBOSA, Diego. Veja como funciona o Centro Integrado de Videomonitoramento inaugurado em Fortaleza: a diferença em relação ao que já existia na Capital é que, agora, a sede tem integração com a Ciops. **Diário do Nordeste**, Fortaleza, 7 abr. 2026. Disponível em: <https://diariodonordeste.verdesmares.com.br/ceara/veja-como-funciona-o-centro-integrado-de-videomonitoramento-inaugurado-em-fortaleza-1.3755580>. Acesso em: 10 abr. 2026.

FREITAS, Juarez. A hermenêutica jurídica e a ciência do cérebro: como lidar com os automatismos mentais. **Revista da AJURIS**, Porto Alegre, v. 40, n. 130, p. 223-244. Disponível em: <https://revistadaajuris.ajuris.org.br/index.php/REVAJURIS/article/view/297/232>. Acesso em: 10 jan. 2026.

FROIS, Catarina. Estudos de vigilância, videovigilância, tecnologia: reflexão sobre o estado da arte. In: CUNHA, Manuela Ivone (ed.). **Do Crime e do Castigo**. Temas e Debates Contemporâneos. Portugal: Mundos Sociais, 2015. p. 147-161.

GARCIA, Emily. Sociedade disciplinar em crise: diálogo entre Foucault, Deleuze e Bloch. **Revista Jurídica Luso-Brasileira**, Lisboa, v. 5, n. 3, p. 523-537, 2019. Disponível em: https://www.cidp.pt/revistas/rjlb/2019/3/2019_03_0523_0537.pdf. Acesso em: 23 set. 2025.

GARFINKEL, Simson. **Database nation: the death of privacy in the 21st century**. Cambridge: O'Reilly, 2001.

GIDDENS, Anthony. **A contemporary critique of historical materialism**. Power, property and the state. London: Macmillan, 1981.

GIDDENS, Anthony. **The Consequences of Modernity**. California: Stanford University Press, 1990.

GIL, Antonio C. **Como Elaborar Projetos de Pesquisa**. 7. ed. Rio de Janeiro: Atlas, 2022. *E-book*. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9786559771653/>. Acesso em: 14 maio 2025.

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

GILLIOM, John; MONAHAN, Torin. **Supervision: An introduction to the surveillance society**. Chicago: The University of Chicago Press, 2013.

GOFFMAN, Erving. **Estigma: notas sobre a manipulação da identidade deteriorada**. 4. ed. Rio de Janeiro: LTC, 1981.

GONZALEZ, Lélia. Racismo e sexismo na cultura brasileira. *In*: RIOS, Flavia; LIMA, Márcia (org.). **Por um feminismo afro-latino-americano**: ensaios, intervenções e diálogos. Rio Janeiro: Zahar, 2020.

GRECO, Luís. **Poder de julgar sem responsabilidade de julgador**: a impossibilidade jurídica do juiz-robô. São Paulo: Marcial Pons, 2020.

GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. **NIST Interagency/Internal Report (NISTIR) 8280** - Face recognition vendor test (FRVT). Part 3: Demographic Effects. Washington: National Institute of Standards and Technology, Department of Commerce, 2019. Disponível em: <https://doi.org/10.6028/NIST.IR.8280>. Acesso em: 15 jan. 2026.

GUREVICH, Yuri. What is an algorithm? *In*: BIELIKOVÁ, M.; FRIEDRICH, G.; GOTTLOB, G.; KATZENBEISSER, S.; TURÁN, G. (ed). **SOFSEM 2012**: Theory and Practice of Computer Science. Lecture Notes in Computer Science, v. 7147. Heidelberg: Springer, 2012. p. 31-42. Disponível em: https://doi.org/10.1007/978-3-642-27660-6_3. Acesso em: 12 abr. 2026.

HAGGERTY, Kevin D.; WILSON, Dean; SMITH, Gavin J. D. Theorizing surveillance in crime control. **Theoretical Criminology**, v. 15, n. 3, p. 231-237, 2011. Disponível em: <https://doi.org/10.1177/1362480610396442>. Acesso em: 25 ago. 2025.

HAMANN, Kristine; SMITH, Rachel. Facial Recognition Technology: Where will it take us. **Criminal Justice**, [S. l.], v. 34, n. 1, p. 9-13, 2019. Disponível em: <https://pceinc.org/wp-content/uploads/2019/11/20190528-Facial-Recognition-Article-3.pdf>. Acesso em: 6 abr. 2026.

HAN, Byung-Chul. **Psicopolítica**: o neoliberalismo e as novas técnicas de poder. Belo Horizonte: Editora Ayiné, 2018.

HARARI, Yuval Noah. **Nexus**: Uma breve história das redes de informação, da Idade da Pedra à inteligência artificial. São Paulo: Companhia das Letras, 2024.

HARDT, Michael. A sociedade mundial de controle. *In*: ALLIEZ, Éric (org.). **Gilles Deleuze**: uma vida filosófica. São Paulo: Ed. 34, 2000. p. 357-372.

HAUSER, Larry. Replies and Rejoinders. *In*: HAUSER, Larry. **Chinese Room Argument**. [S. l.]: Internet Encyclopedia of Philosophy, [s.d.]. Disponível em: <https://iep.utm.edu/chinese-room-argument/#H2>. Acesso em: 10 maio 2026.

HILBERT, Martin. Toward a synthesis of cognitive biases: How noisy information processing can bias human decision making. **Psychological Bulletin**, v. 138, n. 2, p. 211-237, 2012. Disponível em: <https://doi.org/10.1037/a0025940>. Acesso em: 7 jan. 2026.

HINDS, Joanne; WILLIAMS, Emma J.; JOINSON, Adam N. "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. **International Journal of Human-Computer Studies**, v. 143, p. 1-59, 2020. Disponível em: <https://doi.org/10.1016/j.ijhcs.2020.102498>. Acesso em: 30 abr. 2026.

HOBBS, Thomas. **Leviatã, ou Matéria, forma e poder de um estado eclesiástico e civil**. São Paulo: Martin Claret, 2014.

HOFFMANN-RIEM, Wolfgang. Artificial Intelligence as a Challenge for Law and Regulation. In: WISCHMEYER, Thomas; RADEMACHER, Timo (ed.). **Regulating Artificial Intelligence**. Cham: Springer, 2020. p. 1-32.

HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. Tradução de Ítalo Fuhrmann. 2. ed. Rio de Janeiro: Forense, 2022.

HOFSTADTER, Douglas; SANDER, Emmanuel. **Surfaces and essences**: Analogy as the fuel and fire of thinking. New York: Basic Books, 2013.

HOLANDA, Davi. Em debate na Alece, estudiosos pedem mais transparência sobre uso de reconhecimento facial. **Assembleia Legislativa do Estado do Ceará**, 16 abr. 2024. Disponível em: <https://www.al.ce.gov.br/noticias/46072-em-debate-na-alece-estudiosos-pedem-mais-transparencia-sobre-uso-de-reconhecimento-facial>. Acesso em: 16 mar. 2026.

HORTA, Ricardo de Lins e. Por que existem vieses cognitivos na tomada de decisão judicial? A contribuição da psicologia e das neurociências para o debate jurídico. **Revista Brasileira de Políticas Públicas**, Brasília, v. 9, n. 3, p. 83-122, 2019. Disponível em: 10.5102/rbpp.v9i3.6089. Acesso em: 9 jan. 2026.

JAKOBS, Günther. Terroristas como pessoas no direito?. **Novos estudos - CEBRAP**, São Paulo, v. 83, p. 27-36, 2009. Disponível em: <https://doi.org/10.1590/S0101-33002009000100003>. Acesso em: 23 set. 2025.

KAHNEMAN, Daniel. **Rápido e devagar**. Rio de Janeiro: Objetiva, 2012.

KANT, Immanuel. **Resposta à pergunta**: O que é esclarecimento?: E outros textos. São Paulo: Penguin-Companhia, 2022.

KAUFMAN, Dora. Inteligência Artificial: Repensando a mediação. **Brazilian Journal of Development**, Paraná, v. 6, n. 9, p. 67621-67639, 2020. Disponível em: <https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/16481>. Acesso em: 8 jan. 2026.

KELLEHER, John D.; TIERNEY, Brendan. **Data Science**. Cambridge: The MIT Press, 2018.

KELSEN, Hans. **Teoria pura do direito**. 8 ed. São Paulo: WMF Martins Fontes, 2009.

KISSINGER, Henry A.; SCHMIDT, Eric; HUTTENLOCHER, Daniel. **A Era da Inteligência Artificial**: e o nosso futuro humano. Tradução de José Mendonça da Cruz. Alfragide: Editora Dom Quixote, 2022.

KLEINBERG, Jon; LUDWIG, Jens; MULLAINATHAN, Sendhil; SUNSTEIN, Cass R. Discrimination in the Age of Algorithms. **Journal of Legal Analysis**, v. 10, p. 113-174, 2018. Disponível em: <https://doi.org/10.1093/jla/laz001>. Acesso em: 10 jan. 2026.

KOSOFF, Maya. “Senator, I Think We Already Do”: Zuckerberg’s Interrogation Turns into Tech Support. **Vanity Fair**, [S. l.], 11 abr. 2018. Disponível em: https://www.vanityfair.com/news/2018/04/zuckerbergs-interrogation-turns-into-tech-support?srltid=AfmBOopBPkXrlUxQNIJM4rYjIqMa-_X_vBUKZPwiENhTPg9hT7fJdGtg. Acesso em: 30 abr. 2026.

KREMER, Bianca; NUNES, Pablo; LIMA, Thallita G.L. **Racismo algorítmico** [livro eletrônico]. Rio de Janeiro: CESeC, 2023. Disponível em: https://drive.google.com/file/d/1qWb4mPinL2jNTg_A6RLf3BupwpeZPjXl/view. Acesso em: 14 mar. 2026.

LAKATOS, Eva Maria. **Fundamentos de Metodologia Científica**. 9. ed. Rio de Janeiro: Atlas, 2021. *E-book*. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9788597026580/>. Acesso em: 14 maio 2025.

LARSON, Erik J. **The Myth of Artificial Intelligence: why computers can't think the way we do**. Cambridge: Harvard University Press, 2021.

LEITE, Sofia. Racismo estrutural: 87% dos presos no Ceará são pretos ou pardos: o diretor de Pesquisa e Avaliação de Políticas de Segurança Pública da Supesp diz que o problema da associação do povo negro à criminalidade ainda existe. **Diário do Nordeste**, Fortaleza, 30 nov. 2025. Disponível em: <https://diariodonordeste.verdesmares.com.br/seguranca/racismo-estrutural-87-dos-presos-no-ceara-sao-pretos-ou-pardos-1.3714118>. Acesso em: 10 abr. 2026.

LEMERT, Edwin M. **Human deviance, social problems, and social control**. Englewood Cliffs: Prentice Hall, 1967.

LIMA, Paulo Jonas Sales de; FONSÊCA, Felipe Magno Silva. A ausência de tipificação penal na Lei Geral Proteção de Dados: Desafios na persecução penal. **Revista Jurídica do Ministério Público do Estado de Rondônia**, Rondônia, v. 1, n. Especial, p. 168-183, 2025. Disponível em: <https://revista.mpro.mp.br/revistajuridica/article/view/153>. Acesso em: 10 maio 2026.

LINS, Ana Letícia Costa. **Entre pactos, projetos e programas: as dinâmicas de governo no campo da segurança pública no Ceará**. 2020. Dissertação (Mestrado em Sociologia) – Universidade Federal do Ceará, Fortaleza, 2020. Disponível em: <http://repositorio.ufc.br/handle/riufc/56869>. Acesso em: 25 mar. 2026.

LOCKE, John. **Segundo tratado sobre o governo civil e outros escritos**. Petrópolis: Vozes de Bolso, 2019.

LOURENÇO, Luiz. Facções criminosas: um balanço da produção acadêmica no Brasil (2000-2022). **Revista de Ciências Sociais**, Fortaleza, v. 53, n. 3, p. 167-197, 2022. Portal de Periódicos da UFC. Disponível em: <http://dx.doi.org/10.36517/rcs.53.3.d06>. Acesso em: 15 jan. 2026.

LUM, Kristian; ISAAC, William. To predict and serve?. **Significance**, v. 13, n. 5, p. 14-19, 2016. Disponível em: <https://doi.org/10.1111/j.1740-9713.2016.00960.x>. Acesso em: 5 jan. 2026.

LUZ, Paulo Cesar da. Câmeras de reconhecimento facial no Ceará estão funcionando após correções, diz empresa. **ND Mais**, [S. l.], 24 fev. 2026. Disponível em: <https://ndmais.com.br/politica/cameras-de-reconhecimento-facial-no-ceara-estao-funcionando-apos-correcoes/>. Acesso em: 8 abr. 2026.

LYON, David. Cultura da vigilância: envolvimento, exposição e ética na modernidade digital. *In*: BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; GUILHON, Luciana;

MELGAÇO, Lucas (org.). **Tecnopolíticas da vigilância**: perspectivas da margem. São Paulo: Boitempo, 2018. p. 151-179.

LYON, David. **Surveillance as Social Sorting**. New York: Routledge, 2003.

LYON, David. **Surveillance Studies**: An overview. Malden: Polity Press, 2007.

LYON, David. **The Electronic Eye**: The Rise of Surveillance Society. Minneapolis: University of Minnesota Press, 2019.

LYON, David; HAGGERTY, Kevin D.; BALL, Kirstie (ed.). **Introducing surveillance studies**. London: Routledge, 2012. p. 1-11.

MACHADO SEGUNDO, Hugo de Brito. **Direito e inteligência artificial**: o que os algoritmos têm a ensinar sobre interpretação, valores e justiça. São Paulo: Foco, 2023.

MADIEGA, Tambiama; MILDEBRATH, Hendrick. **Regulating facial recognition in the EU**. Directorate-General for Parliamentary Research Services, Brussels, 2021. Disponível em: [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA\(2021\)698021_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf). Acesso em: 4 abr. 2026.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: Editora FGV, 2018.

MAGRO, Diogo Dal; FORTES, Vinícius Borges. O reconhecimento facial nas smart cities e a garantia dos direitos à privacidade e à proteção de dados pessoais. **Revista de Direito Internacional - Brazilian Journal of International Law**, Brasília, v. 18, n. 2, p. 302-329, 2021. Disponível em: <https://doi.org/10.5102/rdi.v18i2.7677>. Acesso em: 7 nov. 2025.

MAIA, Amanda Monique de Souza Aguiar. Decisões algorítmicas na Administração Pública: entre a opacidade técnica e o dever de transparência. **International Journal of Digital Law**, Belo Horizonte, v. 6, e607, p. 3-25, 2025. Disponível em: <https://journal.nuped.com.br/index.php/revista/article/view/1297>. Acesso em: 6 jan. 2026.

MARTINS, Helena; FERREIRA, Katiele; NUNES, Pablo; LIMA, Thalita. **Da construção de uma infraestrutura de vigilância à introdução do reconhecimento facial no Ceará**. Rio de Janeiro: CESeC, 2024. Disponível em: https://cesecseguranca.com.br/wp2025/wp-content/uploads/2025/11/OPANOPTICO_From_the_construction_of_a_surveillance_infrastructure_to_the_introduction_of_face_recognition_in_Ceara.pdf. Acesso em: 16 abr. 2026.

MARX, Gary. What's New About the "New Surveillance"? Classifying for Change and Continuity. **Surveillance and Society**, v. 1, n.1, p. 9-29, 2002. Disponível em: <https://doi.org/10.24908/ss.v1i1.3391>. Acesso em: 23 ago. 2025.

MARX, Paris. **Estrada para lugar nenhum**: o que o vale do silício não entende sobre o futuro dos transportes. São Paulo: Ubu Editora, 2024.

MATIDA, Janaina. Standards de prova: a modéstia necessária a juízes e o abandono da prova por convicção. In: CALDAS, Diana Furtado; ANDRADE, Gabriela Lima; RIOS, Lucas P. Carapiá (org.). **Arquivos da resistência**: ensaios e anais do VII seminário nacional do IBADPP. Florianópolis: Tirant Lo Blanch, 2018. p. 93-110.

MATOS, Mayara, BRAGA, Júlia, CRUZ, Caio, MACHADO, Brenda. **O Programa Cientista Chefe como Política Pública**: análise da implementação. São Paulo: FGV, 2020.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data**: a revolution that will transform how we live, work, and think. Boston: Houghton Mifflin Harcourt; 2013.

MBEMBE, Achille. **Necropolítica**. São Paulo: N-1 Edições, 2018.

MCCARTHY, John. **What is artificial intelligence?**. Stanford, 2000. Disponível em: <http://www-formal.stanford.edu/jmc/whatisai.pdf>. Acesso em: 5 jan. 2026.

MELO, Paulo Victor; SERRA, Paulo. Tecnologia de Reconhecimento Facial e Segurança Pública nas Capitais Brasileiras: Apontamentos e Problematizações. **Comunicação e Sociedade**, v. 42, p. 205-220, 2022. Disponível em: [https://doi.org/10.17231/comsoc.42\(2022\).3984](https://doi.org/10.17231/comsoc.42(2022).3984). Acesso em: 30 ago. 2025.

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

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, Rio de Janeiro, v. 6, n. 2, p. 507-533, 2020. Disponível em: <https://www.estudosinstitucionais.com/REI/article/view/521>. Acesso em: 10 maio 2026.

MENEZES NETO, Elias Jacob de; MORAIS, José Luis Bolzan de. Análises computacionais preditivas como um novo biopoder: modificações do tempo na sociedade dos sensores. **Novos Estudos Jurídicos**, v. 23, n. 3, p. 1129-1154, 2018. Disponível em: <https://doi.org/10.14210/nej.v24n3.p1129-1154>. Acesso em: 30 ago. 2025.

MILLS, Charles. **The racial contract**. New York: Cornell University Press, 1997.

MISSE, Michel. **Crime e violência no Brasil contemporâneo**: estudos de sociologia do crime e da violência urbana. Rio de Janeiro: Lumen Juris, 2006.

MISSE, Michel. Crime, Sujeito e Sujeição criminal: aspectos de uma contribuição analítica sobre a categoria “bandido”. **Revista Lua Nova**, São Paulo, v. 79, p. 15-38, 2010. Disponível em: <https://doi.org/10.1590/S0102-64452010000100003>. Acesso em: 2 abr. 2026.

MISSE, Michel. **Malandros, marginais e vagabundos**: a acumulação social da violência no Rio de Janeiro. 1999. Tese (Doutorado em Sociologia) – Universidade Candido Mendes, Rio de Janeiro, 1999. Disponível em: https://www.researchgate.net/publication/35957970_Malandros_marginais_e_vagabundos_a_acumulacao_social_da_violencia_no_Rio_de_Janeiro. Acesso em: 2 abr. 2026.

MISSE, Michel. Sobre a acumulação social da violência no Rio de Janeiro. **Civitas**: revista de Ciências Sociais, Porto Alegre, v. 8, n. 3, p. 371-385, 2009. Disponível em: <https://revistaseletronicas.pucrs.br/civitas/article/view/4865>. Acesso em: 2 abr. 2026.

MISSE, Michel. Sobre a construção social do crime no Brasil. *In*: MISSE, Michel (org.). **Acusados e acusadores**: estudos sobre ofensas, acusações e incriminações. Rio de Janeiro: Revan, 2008.

MONAHAN, Torin; MURAKAMI-WOOD, David (ed.). **Surveillance Studies: A reader**. New York: Oxford University Press, 2018.

MOREIRA, Adilson José. **Tratado de Direito Antidiscriminatório**. São Paulo: Editora Contracorrente, 2020.

MOROZOV, Evgeny. Digital Technologies And The Future Of Data Capitalism. **Social Europe**, 23 jun. 2015. Disponível em: <https://socialeurope.eu/digital-technologies-and-the-future-of-data-capitalism>. Acesso em: 13 out. 2025.

MOROZOV, Evgeny. **To save Everything, Click Here: The Folly of Technological Solutionism**. New York: PublicAffairs, 2013.

MOROZOV, Evgeny; BRIA, Francesca. **A cidade inteligente: tecnologias urbanas e democracia**. São Paulo: Ubu Editora, 2019.

MOSCHOVAKIS, Yiannis N. What Is an Algorithm? *In*: ENGQUIST, Björn; SCHMID, Wilfried (ed.). **Mathematics Unlimited – 2001 and Beyond**. Heidelberg: Springer Berlin Heidelberg, 2001. p. 919-936.

MURRAY, Daragh; FUSSEY, Pete. Bulk Surveillance in the Digital Age: rethinking the Human Rights law approach to bulk monitoring of communications data. **Israel Law Review**, v. 52, n. 1, p. 31-60, 2019. Disponível em: <https://www.cambridge.org/core/journals/israel-law-review/article/bulk-surveillance-in-the-digital-age-rethinking-the-human-rights-law-approach-to-bulk-monitoring-of-communications-data/AA032EBA3EC3889D27054011853E5E59>. Acesso em: 4 jun. 2026.

NASCIMENTO, Francisco Elionardo de Melo; FREITAS, Geovani Jacó de. Facções, rebeliões, violência e gestão do aprisionamento no Ceará. **O Público e o Privado**, Fortaleza, v. 17, n. 33, p. 143–166, 2019. Disponível em: <https://revistas.uece.br/index.php/opublicoeoprivado/article/view/2261>. Acesso em: 21 abr. 2026.

NEIRA PENA, Ana María. Inteligencia artificial y tutela cautelar. Especial referencia a la prisión provisional. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 7, n. 3, p. 1897-1933, 2021. Disponível em: <https://revista.ibraspp.com.br/RBDPP/article/view/618>. Acesso em: 5 jan. 2026.

NOBLE, Safiya Umoja. **Algorithms of oppression: How search engines reinforce racism**. New York: NYU Press, 2018.

NORRIS, Clive. From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control. *In*: LYON, David (ed.). **Surveillance as Social Sorting: Privacy, risk, and digital discrimination**. New York: Routledge, 2003. p. 249-281.

NUNES, Dierle; LUD, Natanael; PEDRON, Flávio Quinaud. **Desconfiando da imparcialidade dos sujeitos processuais**. Salvador: Juspodivm, 2018.

NUNES, Dierle; MARQUES, Ana Luiza Pinto Coelho. Inteligência artificial e direito processual: vieses algorítmicos e os riscos de atribuição de função decisória às máquinas. **Revista de Processo**, São Paulo, v. 43, n. 285, p. 421-447, 2018. Disponível em: https://www.academia.edu/38112588/Intelig%C3%Aancia_artificial_e_direito_processual_vi

eses_algor%C3%ADmos_e_os_riscos_de_atribui%C3%A7%C3%A3o_de_fun%C3%A7%C3%A3o_decis%C3%B3ria_%C3%A0s_m%C3%A1quinas. Acesso em: 15 mar. 2026.

NUNES, Pablo *et al.* **Maapeando a vigilância biométrica** [livro eletrônico]: levantamento nacional sobre o uso do reconhecimento facial na segurança pública. Rio de Janeiro: CESeC, 2025. Disponível em: https://drive.google.com/file/d/1bN2ssBp_dMiih8YOUonLhGl_5jRoNe5s/view. Acesso em: 10 jan. 2026.

NUNES, Pablo. Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil. *In*: LEMGRUBER, Julita; MUSUMECI, Leonarda; RAMOS, Silvia (coord.). **Retratos da violência**: cinco meses de monitoramento, análises e descobertas. Rio de Janeiro: CESeC, 2019. p. 67-70. Disponível em: https://cesecseguranca.com.br/wp2025/wp-content/uploads/2019/11/Rede-de-Observatorios_primeiro-relatorio_20_11_19.pdf. Acesso em: 11 abr. 2026.

O'NEIL, Cathy. **Weapons of math destruction**: how Big Data increases inequality and threatens democracy. New York: Broadway Books, 2017.

OLIVEIRA SILVA FILHO, Francisco Cláudio; MARIANO, Cynara Monteiro. Fronteiras invisíveis e deslocamentos forçados: impactos da “guerra” de facções na periferia de Fortaleza (Ceará, Brasil). **Revista Direito e Práxis**, Rio de Janeiro, v. 11, n. 3, p. 1548-1570, 2020. Disponível em: <https://www.e-publicacoes.uerj.br/revistaceaju/article/view/43288>. Acesso em: 4 abr. 2026.

OLIVEIRA, Samuel Rodrigues de. **Sorria, você está sendo filmado**: tecnologias de reconhecimento facial, privacidade e proteção de dados. 2020. Dissertação (Mestrado em Direito) – Universidade Federal de Juiz de Fora, Juiz de Fora, 2020. Disponível em: <https://repositorio.ufjf.br/jspui/handle/ufjf/12272>. Acesso em: 2 mar. 2026.

PAIVA, Luiz Fábio Silva. “Aqui não tem gangue, tem facção”: as transformações sociais do crime em Fortaleza. **Caderno CRH**, Salvador, v. 32, n. 85, p. 165-184, 2019. Disponível em: <https://periodicos.ufba.br/index.php/crh/article/view/26375>. Acesso em: 24 mar. 2026.

PAIVA, Luiz Fábio Silva; FREITAS, Geovani Jacó de. Ecos da violência nas margens de uma sociedade democrática: o caso da periferia de Fortaleza. **Sociedade e Cultura**, Goiânia, v. 18, n. 2, 2016. Disponível em: <https://revistas.ufg.br/fcs/article/view/42379>. Acesso em: 3 abr. 2026.

PAIVA, Luiz Fábio. Dinâmicas das violências em tempos de facções criminosas no Ceará: Cada vida importa. *In*: COMITÊ CEARENSE PELA PREVENÇÃO DE HOMICÍDIOS NA ADOLESCÊNCIA. **Relatório do segundo semestre de 2017 do Comitê Cearense pela Prevenção de Homicídios na Adolescência**. Fortaleza: Comitê Cearense pela Prevenção de Homicídios na Adolescência, Governo do Estado do Ceará, 2017. Disponível em: <https://cadavidaimporta.com.br/wp-content/uploads/2018/05/Relato%CC%81rio-2017.2-CORRIGIDO.pdf>. Acesso em: 2 abr. 2026.

PASQUALE, Frank. **The Black Box Society**: The Secret Algorithms That Control Money and Information. Cambridge: Harvard University Press, 2016.

PATZ, Stéfani Reimann. Tecnologias de reconhecimento facial na segurança pública brasileira: impactos, debates e propostas legislativas. *In*: SOUSA, Susana Aires de;

MAGALHÃES, Alberto Raphael Ribeiro; CRESTANI, Ana Cristina; GONÇALVES, Ana; FRANCO, Luiza Cardoso; PÉREZ, María Quintas; FARIAS, Ticiane Teresa Biasutti de (coord.). **Inteligência Artificial e Manutenção da Ordem Pública** [livro eletrônico]: impacto da proposta de Regulamento da IA no direito português. Coimbra: Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, 2024. p. 171-179. Disponível em: <https://doi.org/https://doi.org/10.47907/iaordempublica/livro>. Acesso em: 8 abr. 2026.

PAULO, Lucas Moreschi. Opacidade dos algoritmos e a necessidade de transparência: garantindo explicabilidade. *In*: Seminário Internacional Demandas Sociais e Políticas Públicas na Sociedade Contemporânea, 19, 2023, Santa Cruz do Sul. **Jurisdição Constitucional e Democracia**, Santa Cruz do Sul, 2023, p. 1-20. Disponível em: <https://online.unisc.br/acadnet/anais/index.php/sidspp/article/view/23632>. Acesso em: 5 jan. 2026.

PEER, Eyal; GAMLIEL, Eyal. Heuristics and Biases in Judicial Decisions. **Court Review**, v. 49, n. 2, p. 114-119, 2013. Disponível em: https://digitalcommons.unl.edu/ajacourtreview/422/?utm_source=digitalcommons.unl.edu%2Fajacourtreview%2F422&utm_medium=PDF&utm_campaign=PDFCoverPages. Acesso em: 8 jan. 2026.

PEREIRA, Rui Soares. Sobre o uso de sistemas de identificação biométrica (e de tecnologias de reconhecimento facial) para fins de segurança pública e de aplicação coercitiva da lei: reflexões a propósito da proposta de regulamento europeu sobre a inteligência artificial. **Revista da Faculdade de Direito da Universidade de Lisboa**, v. 63, n. 1-2, p. 839-865, 2022. Disponível em: <http://hdl.handle.net/10451/62137>. Acesso em: 7 abr. 2026.

PERON, Alcides Eduardo dos Reis; ALVAREZ, Marcos César; CAMPELLO, Ricardo Urquiza. Apresentação do dossiê: vigilância, controle e novas tecnologias. **Mediações - Revista de Ciências Sociais**, Londrina, v. 23, n. 1, 2018, p. 11-31, 2018. Disponível em: <https://ojs.uel.br/revistas/uel/index.php/mediacoes/article/view/33884>. Acesso em: 13 out. 2025.

PINHEIRO, Patrícia Peck. **LGPD e GDPR: padrões globais de proteção de dados**. São Paulo: Saraiva, 2020.

PINTO, Nalayne Mendonça. A construção do inimigo: considerações sobre a legislação penal brasileira. **Especiaria: Cadernos de Ciências Humanas**, v. 12, n. 22-23, p. 49-66, 2015. Disponível em: <https://periodicos.uesc.br/index.php/especiaria/article/view/711>. Acesso em: 28 out. 2025.

POGREBINSCHI, Thamy. Foucault, para além do poder disciplinar e do biopoder. **Lua Nova**, v. 63, p. 179-201, 2004. Disponível em: <https://doi.org/10.1590/S0102-64452004000300008>. Acesso em: 23 set. 2025.

POLLI, Frida. The Dark Side Of Artificial Intelligence. **Forbes**, [S. l.], 5 dez. 2017. Disponível em: <https://www.forbes.com/sites/fridapolli/2017/12/05/the-dark-side-of-artificial-intelligence/>. Acesso em: 14 jan. 2026.

PORTELLA, Wilver. Dividual e Subjetivação: formação do indivíduo a partir de retalhos objetivados. **PimentaLab**, 1 jul. 2021. Disponível em: <https://www.pimentalab.net/dividual->

e-subjetivacao-formacao-do-individuo-a-partir-de-retalhos-objetivados/. Acesso em: 3 set. 2025.

PULLEN, Jennifer; SCHEFER, Patricia. Predictive Policing - Grundlagen, Funktionsweise und Wirkung. In: SIMMLER, Monika (ed.). **Smart Criminal Justice: Der Einsatz von Algorithmen in der Polizeiarbeit und Strafrechtspflege**. Basel: Helbing Lichtenhahn Verlag, 2021. p. 103-121. Disponível em: <https://library.oapen.org/handle/20.500.12657/49886>. Acesso em: 10 out. 2025.

QUARESMA, Alexandre. Inteligência artificial e o problema da intencionalidade. **Revista de Tecnología y Sociedad**, v. 10, n. 18, p. 1-26, 2020. Disponível em: <https://doi.org/10.32870/Pk.a10n18.403>. Acesso em: 12 jan. 2026.

RAMOS, Silvia (coord.). **Retratos da Violência – Cinco meses de monitoramento, análises e descobertas**. Rio de Janeiro: CESeC, 2019. Disponível em: https://cesecseguranca.com.br/wp2025/wp-content/uploads/2019/11/Rede-de-Observatorios_primeiro-relatorio_20_11_19.pdf. Acesso em: 3 abr. 2026.

RAMOS, Silvia *et al.* **Pele alvo: a cor que a polícia apaga**. Rio de Janeiro: Rede de Observatórios da Segurança/CESeC, 2022. Disponível em: http://observatorioseguranca.com.br/wordpress/wp-content/uploads/2022/11/EM-EMBARGO-ATE-1711_5-AM-REDE-DE-OBS_PELE-ALVO2_171122.pdf. Acesso em: 20 mar. 2026.

RAMOS, Silvia *et al.* **Pele alvo: crônicas de dor e luta**. Rio de Janeiro: CESeC, 2025. Disponível em: <https://drive.google.com/file/d/1Ahh4JWPRRF-kdfuxBFXYkqLMUJ1MTHZd/view>. Acesso em: 5 abr. 2026.

RAMOS, Silvia *et al.* **Pele alvo: mortes que revelam um padrão**. Rio de Janeiro: CESeC, 2024. Disponível em: https://observatorioseguranca.com.br/wordpress/wp-content/uploads/2024/11/RELATORIO_REDE-DE-OBS_PELE-ALVO-4_web-2.pdf. Acesso em: 4 abr. 2026.

REDMAN, Thomas C. If Your Data Is Bad, Your Machine Learning Tools Are **Useless**. **Harvard Business Review**, [S. l.], 02 abr. 2018. Disponível em: <https://hbr.org/2018/04/if-your-data-is-bad-your-machine-learning-tools-are-useless>. Acesso em: 14 jan. 2026.

REIS, Carolina; ALMEIDA, Eduarda; DA SILVA, Felipe; DOURADO, Fernando. **Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil**. Brasília: Laboratório de Políticas Públicas e Internet, 2021. Disponível em: <https://lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil/>. Acesso em: 15 mar. 2026.

REIS, Sálvio Roberto Freitas. **Desafios no uso de reconhecimento facial em sistemas de vídeo monitoramento no Brasil**. 2025. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Sergipe, São Cristóvão, 2025. Disponível em: <https://ri.ufs.br/handle/riufs/22542>. Acesso em: 16 mar. 2026.

RIBEIRO, Giovana Bellini. Compatibilidade entre a proteção de dados pessoais e o dever de transparência pública. In: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes. **LGPD e Administração Pública: uma análise ampla dos impactos**. São Paulo: Revista dos Tribunais, 2020. p. 293-310.

RIBEIRO, Marcelo da Silva. “**Do tecnosolucionismo ao tecnovigilantismo**”: um estudo sociológico sobre os usos de emergentes tecnologias pelas forças de segurança do Ceará. 2024. Tese (Doutorado em Sociologia) – Universidade Federal do Ceará, Fortaleza, 2024. Disponível em: https://repositorio.ufc.br/bitstream/riufc/78965/3/2024_tese_msribeiro.pdf. Acesso em: 15 mar. 2026.

ROA AVELLA, Marcela del Pilar Roa; SANABRIA-MOYANO, Jesús Eduardo; DINAS-HURTADO, Katherin. Uso del algoritmo COMPAS en el proceso penal y los riesgos a los derechos humanos. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 8, n. 1, p. 275-310, 2022. Disponível em: <https://revista.ibraspp.com.br/RBDPP/article/view/615>. Acesso em: 5 jan. 2026.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

ROSA, Pablo Ornelas; LEMOS, Clécio José Morandi de Assis; SOUZA, Aknaton Toczec; BENTO, Eudson Ferreira. Efeitos da biometria na segurança pública brasileira: uma análise sobre reconhecimento facial e racismo algoritmo. **Revista de Geopolítica**, Paraná, v. 16, n. 5, p. e997, 2025. Disponível em: <https://revistageo.com.br/revgeo/article/view/997>. Acesso em: 2 abr. 2026.

ROUSSEAU, Jean-Jacques. **O Contrato Social**: Princípios do Direito Político. São Paulo: Edipro, 2017.

ROUVROY, Antoinette; BERNS, Thomas. Gouvernamentalité algorithmique et perspectives d'émancipation: Le disparate comme condition d'individuation par la relation ? **Réseaux**, v.1, n. 177, p. 163-196, 2013. Disponível em: <https://doi.org/10.3917/res.177.0163>. Acesso em: 13 out. 2025.

ROUVROY, Antoinette; BERNS, Thomas. Le nouveau Pouvoir Statistique: ou quand le contrôle s'exerce sur un réel normé, docile et sans événement car constitué de corps “numériques”. **Multitudes**, n. 40, p. 88-103, 2010. Disponível em: <https://doi.org/10.3917/mult.040.0088>. Acesso em: 13 out. 2025.

RUDIN, Cynthia. Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. **Nature Machine Intelligence**, v. 1, p. 206-215, 2019. Disponível em: <https://doi.org/10.1038/s42256-019-0048-x>. Acesso em: 4 jan. 2026.

RULE, James B. **Private Lives and Public Surveillance**: Social Control in the Computer Age. New York: Schocken Books Inc, 1974.

RUSSELL, Stuart; NORVIG, Peter. **Artificial Intelligence**: a modern approach. 3. ed. New Jersey: Prentice Hall, 2010.

SABOT, Philippe. O que é uma sociedade disciplinar? Gênese e atualidade de um conceito, a partir de Vigiar e Punir. **DoisPontos**, Curitiba, v. 14, n. 1, p. 15-27, 2017. Disponível em: <https://doi.org/10.5380/dp.v14i1.56536>. Acesso em: 24 set. 2025.

SANTAELLA, Rodrigo. Inteligência Artificial na Terra do Sol: um olhar global desde o Ceará. In: PARANÁ, Edemilson; SANTAELLA, Rodrigo (org.). **Estado e inteligência artificial**: o caminho brasileiro e os usos cearenses. EdUECE: Fortaleza, 2025. p. 8-15.

Disponível em: <https://www.uece.br/eduece/wp-content/uploads/sites/88/2025/10/Estado-e-Intelig%C3%Aancia-Artificial-o-caminho-brasileiro-e-os-usos-cearenses.pdf>. Acesso em: 4 maio 2026.

SANTANA, Rafael da Silva. A necessidade como elemento modulador da validade dos atos de tratamento de dados pessoais. In: REQUIÃO, Maurício (org.). **Proteção de dados pessoais: novas perspectivas**. Salvador: EDUFBA, 2022. p. 84-104. Disponível em: <https://repositorio.ufba.br/bitstream/ri/35799/3/protecao-de-dados-pessoais-RI.pdf>. Acesso em: 9 maio 2026.

SANTINI, R. Marie; SALLES, Débora; MATTOS, Bruno; SANCHOTENE, Nicole; HADDAD, João Gabriel; SILVA, Daphne; BORGES, Amanda; YONESHIGUE, Bernardo; DAU, Erick; BENZECRY, Lena. **O ‘chilling effect’ em debate: a moderação de conteúdo nas plataformas digitais após regulação na Europa**. Rio de Janeiro: NetLab – Laboratório de Estudos de Internet e Redes Sociais, Universidade Federal do Rio de Janeiro, 2025. Disponível em: 10.13140/RG.2.2.10466.03529. Acesso em: 18 jan. 2026.

SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**. 11. ed. Porto Alegre: Livraria do Advogado, 2012.

SCHLITTLER, Maria Carolina de Camargo. **Matar muito, prender mal: a produção da desigualdade racial como efeito do policiamento ostensivo militarizado em SP**. 2016. Tese (Doutorado em Sociologia) – Universidade Federal de São Carlos, São Carlos, 2016. Disponível em: <https://repositorio.ufscar.br/server/api/core/bitstreams/988924cb-3b19-4ec7-8437-12e87e00cd3a/content>. Acesso em: 5 maio 2026.

SEARLE, John. **A Redescoberta da Mente**. São Paulo: Martins Fontes, 2006.

SEYFERTH, Giralda. Colonização, imigração e a questão racial no Brasil. **Revista USP**, São Paulo, n. 53, p. 117-149, 2002. Disponível em: <https://revistas.usp.br/revusp/article/view/33192>. Acesso em: 2 abr. 2026.

SHUBIK, Martin. **Teoría de Juegos en las Ciencias Sociales: conceptos e soluciones**. México: Fondo de Cultura Económica de España, 1992.

SILVA, Caroline Cordeiro Viana e; PEREIRA, Alexsandro Eugenio. A Teoria de Securitização e a sua aplicação em artigos publicados em periódicos científicos. **Revista de Sociologia e Política**, v. 27, n. 69, p. 1-20, 2019. Disponível em: <https://doi.org/10.1590/1678987319276907>. Acesso em: 28 out. 2025.

SILVA, Lucas Lucena da; XAVIER, Antônio Roberto. O projeto “Identifica Ceará” como política pública de segurança pública de prevenção e combate ao crime. **Revista Políticas Públicas & Cidades**, Curitiba, v. 14, n. 4, p. 1-16, 2025. Disponível em: <https://journalppc.com/RPPC/article/view/2001>. Acesso em: 2 abr. 2026.

SILVA, Paulo Henrique Moura da. Desenvolvimento tecnológico recente da segurança pública do Ceará por meio da inteligência artificial: a construção de um ecossistema tecnológico. In: PARANÁ, Edemilson; SANTAELLA, Rodrigo (org.). **Estado e inteligência artificial: o caminho brasileiro e os usos cearenses**. Fortaleza: EdUECE, 2025a. p. 78-111. Disponível em: <https://www.uece.br/eduece/wp-content/uploads/sites/88/2025/10/Estado-e-Intelig%C3%Aancia-Artificial-o-caminho-brasileiro-e-os-usos-cearenses.pdf>.

Intelig%C3%Aancia-Artificial-o-caminho-brasileiro-e-os-usos-cearenses.pdf. Acesso em: 4 maio 2026.

SILVA, Rosane Leal da; SILVA, Fernanda dos Santos Rodrigues da. Reconhecimento facial e segurança pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro. *In*: 5 Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede, 5., 2019, Santa Maria. **Anais [...]** Santa Maria: UFSM, 2019. Disponível em: <https://www.ufsm.br/app/uploads/sites/563/2019/09/5.23.pdf>. Acesso em: 3 abr. 2026.

SILVA, Tarcízio. **Racismo algorítmico**: Inteligência artificial e discriminação nas redes digitais. Edições Sesc: São Paulo, 2024.

SILVA, Wanessa Rezende. **Privacidade sob vigilância estatal**: entre a proteção de dados e os interesses da segurança pública. 2025. Dissertação (Mestrado em Direito Econômico e Desenvolvimento) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, DF, 2025b. Disponível em: <https://repositorio.idp.edu.br/handle/123456789/5547>. Acesso em: 9 maio 2026.

SIMON, Herbert. Designing organizations for an information-rich world. *In*: GREENBERGER, Martin (ed.). **Computers, Communication, and the Public Interest**. Baltimore: Johns Hopkins Press, 1971.

SMITH, Craig. Dealing With Bias in Artificial Intelligence. **The New York Times**. New York, 19 nov. 2019. Disponível em: https://www.nytimes.com/2019/11/19/technology/artificial-intelligence-bias.html?fbclid=IwAR2nyAo-nFfh-H6P0XwYsGq0pZ4tXFpV1vPIMxE_Ztea1nJ7dAmsTqL96Uk. Acesso em: 14 jan. 2026.

SOLAROVA, Sara; PODROUŽEK, Juraj; MESARČÍK, Matúš; GAVORNIK, Adrian; BIELIKOVA, Maria. Reconsidering the regulation of facial recognition in public spaces. **AI and Ethics**, v. 3, n. 2, p. 625-635, 2023. Disponível em: <https://doi.org/10.1007/s43681-022-00194-0>. Acesso em: 16 mar. 2026.

SOUZA, Carlos Affonso Pereira de; VIOLA, Mario; PADRÃO, Vinicius. Considerações iniciais sobre os interesses legítimos do controlador na Lei Geral de Proteção de Dados Pessoais. **Revista Direito Público**, Porto Alegre, v. 16, n. 90, 2019, p. 109-131. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3744>. Acesso em: 10 maio 2026.

SOUZA, Letícia Vitoria Rodrigues Lima de; RIBEIRO, Juliana Campos de Aguiar Mattos; BANCHIK, Antonio Mario. A controvérsia da utilização de Tecnologias de Reconhecimento Facial no Brasil. **Encontro EDICIC Ibérico**, Porto, v. 11, p. 1-13, 2026. Disponível em: <https://doi.org/10.34630/xiedicic.vi.6707>. Acesso em: 8 abr. 2026.

SOUZA, Michel R. O.; ZANATTA, Rafael A. F. The problem of automated facial recognition technologies in Brazil: social countermovements and the new frontiers of fundamental rights. **Latin American Human Rights Studies**, v. 1, p. 1-34, 2021. Disponível em: <https://revistas.ufg.br/lahrs/article/view/69423>. Acesso em: 5 jan. 2025.

TAVARES, João Paulo Lordelo Guimarães. Vieses implícitos e técnicas de automação decisória: riscos e benefícios. **Civil Procedure Review**, Salvador, v. 12, n. 1, p. 105-132,

2021. Disponível em: <https://www.civilprocedurereview.com/revista/article/view/225>. Acesso em: 24 jan. 2026.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**, Rio de Janeiro, v. 9, n. 1, p. 1-38, 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/510>. Acesso em: 9 maio 2026.

TÉLLEZ CARVAJAL, Evelyn. Análisis documental sobre el tema del big data y su impacto en los derechos humanos. **Derecho PUCP**, Lima, n. 84, p. 155-188, 2020. Disponível em: <https://revistas.pucp.edu.pe/index.php/derechopucp/article/view/22109>. Acesso em: 8 jan. 2026.

TONETTO, Leandro Miletto; KALIL, Lisiane Lindenmeyer; MELO, Wilson Vieira; SCHNEIDER, Daniela Di Giorgio; STEIN, Lilian Milnitsky. O papel das heurísticas no julgamento e na tomada de decisão sob incerteza. **Estudos de Psicologia**, Campinas, v. 23, n. 2, p. 181-189, 2006. Disponível em: <https://periodicos.puc-campinas.edu.br/estpsi/article/view/6791>. Acesso em: 24 jan. 2026.

TVERSKY, Amos; KAHNEMAN, Daniel. Julgamento sob incerteza: heurísticas e vieses. *In*: KAHNEMAN, Daniel. **Rápido e devagar**. Rio de Janeiro: Objetiva, 2012. Apêndice A, p. 524-539.

UTSET, Manuel A. Predictive policing and criminal law. *In*: MCDANIEL, John; PEASE, Ken (ed.). **Predictive Policing and Artificial Intelligence**. New York: Routledge, 2021, p. 163-182.

VASCONCELLOS, Vinicius Gomes de. Standard probatório para condenação e dúvida razoável no processo penal: análise das possíveis contribuições ao ordenamento brasileiro. **Revista Direito GV**, São Paulo, v. 16, n. 2, p. 1-26, 2020. Disponível em: <https://doi.org/10.1590/2317-6172201961>. Acesso em: 5 maio 2026.

VEGA, Ignacio Gonzalez. Desafíos y riesgos en la aplicación de la IA en el Poder Judicial. *In*: HERNÁNDEZ, Fátima Mateos (coord.). **Boletín de Inteligencia Artificial**. Vol. IV. Madrid: Juezas y Jueces para la Democracia, 2025, p. 8-13. Disponível em: <https://www.juecesdemocracia.es/2025/06/15/boletin-de-inteligencia-artificial-volumen-iv/>. Acesso em: 3 jan. 2026.

VIANA, Antonio Aurelia de Souza. O juiz-robô e o crepúsculo da atividade decisória humana. **Publicação Contínua**, v. 6, p. 1-25, 2021. Disponível em: <https://doi.org/10.21875/tjc.v6i0.44813>. Acesso em: 5 jan. 2026.

VON NEUMANN, John; MORGENSTERN, Oskar. **Theory of Games and Economic Behavior**. Princeton: Princeton University Press, 1953.

WANG, Jackie. **Capitalismo Carcerário**. Tradução de Bruno Xavier. São Paulo: Igra Kniga, 2022.

WEISBURD, David; TELEP, Cody W. Hot Spots Policing: What We Know and What We Need to Know. **Journal of Contemporary Criminal Justice**, v. 30, n. 2, p. 200-220, 2014. Disponível em: <https://doi.org/10.1177/1043986214525083>. Acesso em: 3 jan. 2026.

WELLER, Toni. The information state: An historical perspective on Surveillance. *In*: BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David (ed.). **The Routledge Handbook of Surveillance Studies**. New York: Routledge, 2012. p. 57-63.

WELSH, Brandon C.; FARRINGTON, David P. Effects of Closed Circuit Television Surveillance on Crime. **Campbell Systematic Reviews**, v. 4, n. 1, p. 1-73, 2008. Disponível em: <https://doi.org/10.4073/csr.2008.17>. Acesso em: 17 out. 2025.

ZENG, Jinhua; QIU, Xiulian; SHI, Shaopei. Image processing effects on the deep face recognition system. **Math Biosci Eng**, [S. l.], v. 18, n. 2, p. 1187-1200, 2021. Disponível em: [10.3934/mbe.2021064](https://doi.org/10.3934/mbe.2021064). Acesso em: 18 mar. 2026.

ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para a civilização de informação. *In*: BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; GUILHON, Luciana; MELGAÇO, Lucas (org.). **Tecnopolíticas da vigilância: perspectivas da margem**. São Paulo: Boitempo, 2018. p. 17-68.