

O PANÓPTICO DIGITAL: NOVAS TECNOLOGIAS COMO FERRAMENTAS DE CONTROLE SOCIAL E SEUS REFLEXOS NO DIREITO PENAL

Déa Carla Pereira Nery



<https://doi.org/10.36557/2674-9432.2026v5n3p2500-2512>

Artigo recebido em 25 de Março e publicado em 25 de Maio de 2026

ARTIGO ORIGINAL

RESUMO

O presente artigo analisa a intersecção entre controle social, direito penal e o uso de novas tecnologias na sociedade da informação. A partir de uma abordagem crítico-metodológica, investiga-se como ferramentas tecnológicas, a exemplo da inteligência artificial, reconhecimento facial e policiamento preditivo, têm reconfigurado as dinâmicas de vigilância e controle punitivo. O objetivo central é compreender de que maneira a digitalização do controle social afeta as garantias fundamentais e potencializa a seletividade do sistema de justiça criminal. A pesquisa, de natureza bibliográfica e documental, demonstra que a transição de um modelo disciplinar clássico para um controle algorítmico difuso cria um 'panóptico digital', no qual a coleta massiva de dados atua como mecanismo de prevenção e repressão de condutas. Conclui-se que, embora as inovações tecnológicas ofereçam promessas de eficiência na segurança pública, elas frequentemente reproduzem vieses discriminatórios e operam à margem do devido processo legal, exigindo uma releitura da dogmática penal e a construção de limites ético-jurídicos rigorosos para conter o avanço do autoritarismo tecnológico.

Palavras-chave: Controle social, Direito penal, Novas tecnologias, Policiamento preditivo, Vigilância algorítmica.

ABSTRACT

This article analyzes the intersection between social control, criminal law, and the use of new technologies in the information society. From a critical-methodological approach, it investigates how technological tools, such as artificial intelligence, facial recognition, and predictive policing, have reconfigured the dynamics of surveillance and punitive control. The main objective is to understand how the digitalization of social control affects fundamental guarantees and enhances the selectivity of the criminal justice system. The research, of a bibliographic and documentary nature, demonstrates that the transition from a classical disciplinary model to diffuse algorithmic control creates a 'digital panopticon', in which massive data collection acts as a mechanism for the prevention and repression of conduct. It concludes that, although technological innovations offer promises of efficiency in public security, they frequently reproduce discriminatory biases and operate outside due process of law, requiring a rereading of criminal dogmatics and the construction of strict ethical-legal limits to contain the advance of technological authoritarianism.

Keywords: Social control, Criminal law, New technologies, Predictive policing, Algorithmic surveillance.

Instituição afiliada – Doutora e Mestre em Direito/PUC/SP. Mestre em Criminologia/UPO/Espanha. Professora Adjunta da UNEB(Universidade do Estado da Bahia).

Autor correspondente: *Déa Carla Pereira Nery*

This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).



1 INTRODUÇÃO

A sociedade contemporânea vivencia uma transformação paradigmática impulsionada pelo avanço exponencial das tecnologias de informação e comunicação. A digitalização das relações sociais, a coleta massiva de dados (Big Data) e o desenvolvimento de sistemas de inteligência artificial reconfiguraram não apenas a economia e a cultura, mas também as estruturas de poder e os mecanismos de controle social. O advento da chamada Quarta Revolução Industrial trouxe consigo ferramentas capazes de processar volumes inimagináveis de informações em tempo real, alterando substancialmente a forma como o State interage com os cidadãos e exerce seu poder de polícia.

Historicamente, o Direito Penal tem operado como a ultima ratio do controle social formal, atuando na repressão de condutas consideradas gravemente lesivas aos bens jurídicos tutelados pelo Estado. No entanto, a emergência de novas tecnologias tem deslocado o eixo de atuação do sistema de justiça criminal, promovendo uma transição de um modelo reativo e punitivo para um paradigma preventivo e atuarial, centrado na gestão de riscos e na predição de comportamentos. Essa mudança de paradigma reflete uma nova racionalidade governamental, na qual a antecipação do crime torna-se mais relevante do que a punição do infrator após o cometimento do delito.

Nesse contexto, ferramentas como o policiamento preditivo, o reconhecimento facial e a vigilância algorítmica emergem como novos instrumentos de controle social. Sob a justificativa de otimizar a segurança pública e reduzir os índices de criminalidade, o Estado passa a adotar aparatos tecnológicos que permitem um monitoramento contínuo e ubíquo dos cidadãos, instaurando o que a doutrina tem denominado de 'panóptico digital'. A promessa de uma segurança pública baseada em dados e algoritmos seduz gestores públicos e a própria sociedade, frequentemente amedrontada pelo aumento da criminalidade urbana e pela sensação de insegurança.

O presente artigo tem como objetivo analisar os impactos dessas novas tecnologias no âmbito do controle social e do Direito Penal. A problemática central que orienta a pesquisa consiste em investigar em que medida a utilização de ferramentas tecnológicas para fins de segurança pública afeta as garantias fundamentais dos indivíduos e potencializa a seletividade inerente ao sistema penal. Questiona-se, fundamentalmente, se a incorporação acrítica dessas tecnologias pelo sistema de justiça criminal não estaria promovendo uma erosão silenciosa dos princípios garantistas que estruturam o Estado Democrático de Direito.

A relevância deste estudo reside na necessidade urgente de debater os limites éticos e jurídicos da atuação estatal na era digital, especialmente diante da ausência de marcos regulatórios específicos para o uso de inteligência artificial na segurança pública brasileira. Como professora e pesquisadora da Universidade do Estado da Bahia (UNEB), busco contribuir para a construção de uma dogmática penal crítica, capaz de responder aos desafios da modernidade tecnológica sem abrir mão das conquistas democráticas e dos direitos fundamentais.

2 METODOLOGIA

Para a consecução dos objetivos propostos, este trabalho adota uma metodologia de natureza qualitativa, pautada na pesquisa bibliográfica e documental, com uma abordagem crítico-reflexiva. O referencial teórico foi construído a partir da revisão de literatura nacional e estrangeira de referência nas áreas de criminologia crítica, sociologia do controle, direito penal, direito processual penal e regulação de novas tecnologias.

A pesquisa documental compreendeu a análise de relatórios de organizações da sociedade civil sobre o uso de tecnologias de vigilância no Brasil, dados estatísticos sobre a implementação de sistemas de reconhecimento facial e decisões judiciais relevantes que abordam a temática. A seleção das fontes bibliográficas priorizou autores clássicos e contemporâneos que discutem as transformações do controle social, tais como Michel Foucault, Gilles Deleuze, Shoshana Zuboff, David Garland e Cathy O'Neil.

O método de abordagem crítico-reflexivo permitiu desvelar as tensões existentes entre a busca por eficiência e modernização na segurança pública e a imperiosa necessidade de preservação dos direitos e garantias fundamentais consagrados na Constituição Federal de 1988. A análise estruturou-se em três etapas principais: (i) reconstrução histórica e conceitual do controle social e sua relação com o Direito Penal; (ii) investigação do impacto da revolução tecnológica e da governança algorítmica na configuração da sociedade da informação; e (iii) análise crítica das ferramentas específicas de controle penal (policiamento preditivo e reconhecimento facial) e seus reflexos na seletividade e nas garantias processuais.

3 RESULTADOS e DISCUSSÃO

3.1 Controle Social e Direito Penal na Modernidade: Do Panóptico à Sociedade de Controle

O conceito de controle social é fundamental para a compreensão das dinâmicas de organização e manutenção da ordem nas sociedades humanas. Em termos sociológicos, o controle social abrange o conjunto de mecanismos, estratégias e sanções por meio dos quais uma coletividade busca assegurar a conformidade de seus membros às normas, valores e expectativas dominantes. Trata-se de um processo contínuo de socialização e coerção que visa neutralizar os comportamentos desviantes e garantir a coesão social.

A teoria sociológica tradicional distingue o controle social informal do controle social formal. O primeiro é exercido por instituições primárias, como a família, a escola, a religião e os grupos de pares, operando por meio de processos de socialização e internalização de regras. O controle informal atua de maneira sutil e difusa, moldando as consciências e os comportamentos desde a infância. O segundo, por sua vez, é exercido pelo Estado e suas agências especializadas (polícia, ministério público,

judiciário, sistema prisional), entrando em ação quando as instâncias informais falham em conter o comportamento desviante.

O Direito Penal insere-se no âmbito do controle social formal, caracterizando-se como o instrumento mais drástico e invasivo de que dispõe o Estado. Sua atuação é pautada pela imposição de sanções punitivas, notadamente a privação de liberdade, àqueles que transgridem as normas penais. Contudo, a criminologia crítica tem demonstrado que o sistema penal não opera de forma neutra ou igualitária; ao contrário, ele é estruturalmente seletivo, recaindo de maneira desproporcional sobre determinados grupos sociais, geralmente os mais vulneráveis e marginalizados (ANDRADE, 2003; ZAFFARONI, 1991).

Na modernidade, a consolidação do Estado-nação e o desenvolvimento do capitalismo industrial demandaram novas formas de disciplina e controle dos corpos. Michel Foucault (2014), em sua obra clássica *Vigiar e Punir*, descreve a transição dos suplícios públicos para o modelo disciplinar, simbolizado pela prisão e arquitetonicamente representado pelo panóptico de Jeremy Bentham. O panoptismo institui uma vigilância invisível e onipresente, induzindo o indivíduo a um estado de permanente visibilidade que assegura o funcionamento automático do poder.

O panóptico benthamiano, concebido no final do século XVIII, consistia em uma estrutura arquitetônica circular com uma torre de vigilância no centro e celas na periferia. O vigilante na torre podia observar todos os detentos, mas estes não podiam ver o vigilante. Essa assimetria visual criava a ilusão de uma vigilância constante, levando os indivíduos a internalizarem a disciplina e a se autovigiarem. Foucault utilizou essa metáfora para descrever o funcionamento das instituições disciplinares modernas, como prisões, escolas, hospitais e fábricas.

No entanto, as transformações sociais, econômicas e tecnológicas das últimas décadas indicam o esgotamento do modelo disciplinar clássico. Gilles Deleuze (1992), dialogando com a obra de Foucault, propôs o conceito de 'sociedades de controle', nas quais a disciplina exercida em espaços fechados cede lugar a mecanismos de controle contínuos, abertos e fluidos, viabilizados pelas tecnologias de informação. Nas sociedades de controle, o poder não opera mais predominantemente pelo confinamento físico, mas pela modulação dos fluxos de informação e pela gestão dos acessos.

Nesse novo paradigma, o controle não se dá apenas pela coerção física ou pelo confinamento, mas pela modulação de comportamentos, pelo rastreamento de fluxos e pela gestão de dados. O indivíduo torna-se um 'dividual', uma entidade fragmentada em senhas, perfis, scores e metadados, que são constantemente monitorados e avaliados por sistemas informáticos. A vigilância deixa de ser localizada e episódica para se tornar ubíqua e contínua, acompanhando o indivíduo em todos os momentos de sua vida.

É nesse contexto de transição que o Direito Penal e as agências de segurança pública passam a incorporar novas tecnologias como ferramentas centrais de controle social. A racionalidade penal moderna, baseada na culpabilidade individual e na retribuição proporcional ao dano causado, entra em tensão com a racionalidade atuarial das novas tecnologias, que prioriza a identificação de grupos de risco e a intervenção preventiva (GARLAND, 2008; HARCOURT, 2007). Essa mudança de foco tem profundas implicações para a dogmática penal e para a proteção dos direitos fundamentais.

3.2 A Revolução Tecnológica, o Capitalismo de Vigilância e a Governança Algorítmica

A virada para o século XXI foi marcada por uma revolução tecnológica sem precedentes, caracterizada pela convergência entre computação, telecomunicações e biotecnologia. A disseminação da internet, a proliferação de dispositivos móveis e o advento da 'Internet das Coisas' (IoT) conectaram pessoas, objetos e instituições em uma rede global, dando origem ao que Manuel Castells (1999) denominou de 'sociedade em rede'. Essa nova morfologia social é estruturada em torno de fluxos de informação que transcendem as fronteiras geográficas e temporais.

Nessa nova configuração social, a informação e o conhecimento tornam-se os principais ativos econômicos e fontes de poder. A capacidade de coletar, processar e analisar volumes massivos de dados (Big Data) em tempo real transformou radicalmente os modelos de negócios, a governança pública e as interações cotidianas. O Big Data caracteriza-se pelos 'Três Vs': volume (quantidade massiva de dados), velocidade (geração e processamento em tempo real) e variedade (diversidade de formatos e fontes de dados).

Shoshana Zuboff (2020) cunhou a expressão 'capitalismo de vigilância' para descrever a lógica econômica baseada na extração e mercantilização de dados comportamentais, visando à predição e modificação de condutas humanas. Nesse modelo, a experiência humana gratuita é apropriada como matéria-prima para a extração de dados, que são processados por algoritmos de inteligência artificial para gerar produtos preditivos. Esses produtos são então vendidos em mercados de futuros comportamentais, onde empresas pagam para prever e influenciar as ações dos consumidores.

A sociedade da informação é, intrinsecamente, uma sociedade da vigilância. A cada interação digital – seja uma busca na web, uma compra online, uma postagem em rede social ou o simples deslocamento com um smartphone no bolso – os indivíduos deixam rastros digitais que são capturados, armazenados e processados por algoritmos. Essa 'datificação' da vida cotidiana cria um espelho digital de cada pessoa, revelando suas preferências, hábitos, vulnerabilidades e redes de relacionamento. A privacidade, outrora considerada um direito fundamental inalienável, passa a ser tratada como uma mercadoria negociável em troca de serviços digitais 'gratuitos'.

O desenvolvimento da inteligência artificial (IA), especialmente das técnicas de aprendizado de máquina (machine learning), potencializou exponencialmente a

capacidade de extrair sentido desse oceano de dados. Sistemas de IA são capazes de identificar padrões complexos, estabelecer correlações ocultas e formular previsões com alto grau de precisão. Diferentemente da programação tradicional, na qual as regras são explicitamente definidas por humanos, o aprendizado de máquina permite que os algoritmos 'aprendam' a partir dos dados, ajustando seus modelos internos de forma autônoma.

Essa capacidade analítica tem sido amplamente apropriada pelo Estado para fins de segurança pública e controle social. A transição para a governança algorítmica implica uma mudança na racionalidade do controle. Enquanto o modelo tradicional baseava-se na suspeita individualizada e na investigação de fatos passados, o novo modelo orienta-se pela análise de risco, pela probabilidade e pela antecipação de eventos futuros. A lógica atuarial, antes restrita ao setor de seguros, passa a colonizar o sistema de justiça criminal, transformando a segurança pública em um exercício de gestão de riscos populacionais.

Nesse cenário, a presunção de inocência cede espaço a uma presunção de risco generalizada. Todos os cidadãos tornam-se, em alguma medida, suspeitos em potencial, cujos dados devem ser continuamente monitorados e avaliados por sistemas automatizados. A vigilância deixa de ser uma medida excepcional, justificada por indícios concretos de autoria e materialidade delitiva, para se tornar a regra, o estado padrão de funcionamento da sociedade conectada. O panóptico digital, diferentemente do panóptico arquitetônico, não exige o confinamento físico; ele opera de forma invisível e capilarizada, infiltrando-se nos interstícios da vida cotidiana.

3.3 Novas Tecnologias como Ferramentas de Controle Social Penal

A incorporação de novas tecnologias pelas agências de segurança pública e pelo sistema de justiça criminal tem reconfigurado profundamente as práticas de controle social penal. Sob o discurso da modernização, da eficiência e da neutralidade tecnológica, o Estado tem adotado uma série de ferramentas que ampliam sua capacidade de vigilância e intervenção. Destacam-se, nesse contexto, o policiamento preditivo e os sistemas de reconhecimento facial, que representam a vanguarda da aplicação da inteligência artificial na esfera penal.

3.3.1 Vigilância Algorítmica e Policiamento Preditivo

O policiamento preditivo (predictive policing) consiste na utilização de algoritmos e análises de Big Data para prever onde, quando e por quem crimes têm maior probabilidade de ocorrer, orientando a alocação de recursos policiais e as estratégias de patrulhamento. Essa tecnologia baseia-se na premissa de que o comportamento criminal não é aleatório, mas segue padrões espaciais e temporais que podem ser identificados por modelos matemáticos. A promessa é a de que a polícia possa atuar de forma proativa, prevenindo a ocorrência de delitos antes mesmo que eles aconteçam.

Existem, fundamentalmente, duas modalidades de policiamento preditivo: a predição baseada em locais (place-based) e a predição baseada em pessoas (person-based). A primeira utiliza dados históricos de criminalidade para identificar 'zonas quentes' (hotspots) com maior risco de ocorrência de delitos, direcionando o patrulhamento ostensivo para essas áreas. Softwares como o PredPol (agora Geolitica) tornaram-se populares em diversas cidades ao redor do mundo, prometendo otimizar o uso do efetivo policial e reduzir as taxas de criminalidade patrimonial.

A segunda modalidade, mais controversa, busca identificar indivíduos com maior probabilidade de se envolverem em atividades criminosas, seja como autores ou como vítimas, a partir da análise de seus antecedentes, redes de relacionamento e comportamentos. Programas como o 'Strategic Subject List' (SSL) do Departamento de Polícia de Chicago geraram intensos debates sobre a legalidade e a ética de se atribuir 'pontuações de risco' a cidadãos com base em algoritmos opacos. A predição baseada em pessoas aproxima-se perigosamente do conceito de 'direito penal do autor', punindo o indivíduo não pelo que ele fez, mas pelo que ele supostamente é ou pode vir a fazer.

Embora os defensores do policiamento preditivo argumentem que a tecnologia permite uma atuação policial mais objetiva e eficiente, críticos apontam para o risco de reprodução e amplificação de vieses discriminatórios. Os algoritmos são treinados com base em dados históricos produzidos pelas próprias agências policiais, os quais refletem as práticas de policiamento do passado. Se a polícia historicamente concentrou suas abordagens em bairros periféricos e populações marginalizadas, os dados refletirão uma maior incidência criminal nessas áreas, levando o algoritmo a prever mais crimes nesses mesmos locais.

Cria-se, assim, um ciclo vicioso de feedback (feedback loop): o algoritmo direciona a polícia para áreas vulneráveis; a maior presença policial resulta em mais abordagens e prisões (frequentemente por crimes de menor potencial ofensivo, como posse de drogas); essas novas prisões alimentam o banco de dados, confirmando a predição inicial e justificando o envio de ainda mais policiais para a região. O resultado é a hipervigilância e a supercriminalização de grupos historicamente estigmatizados, sob o verniz de uma suposta neutralidade matemática. A tecnologia, longe de eliminar o viés humano, atua como um mecanismo de 'lavagem algorítmica' (mathwashing), conferindo uma aura de objetividade científica a práticas discriminatórias (O'NEIL, 2016).

Além disso, a opacidade dos algoritmos (o chamado problema da 'caixa preta') dificulta o escrutínio público e o controle de legalidade sobre as decisões automatizadas. Muitas dessas ferramentas são desenvolvidas por empresas privadas e protegidas por segredo comercial, impedindo que os cidadãos e até mesmo os operadores do direito compreendam os critérios utilizados para classificar uma área ou um indivíduo como 'de alto risco'. A impossibilidade de auditar o código-fonte e os dados de treinamento compromete o princípio da transparência e inviabiliza o exercício do contraditório e da ampla defesa.

3.3.2 Reconhecimento Facial e Seletividade Penal

Outra tecnologia que tem ganhado destaque como ferramenta de controle social é o reconhecimento facial automatizado. Esses sistemas utilizam inteligência artificial para mapear características biométricas da face humana capturadas por câmeras de vigilância, comparando-as em tempo real com bancos de dados de pessoas procuradas, foragidos ou suspeitos. A promessa de identificar criminosos em meio a multidões tem impulsionado a adoção dessa tecnologia por governos em todo o mundo, frequentemente associada a projetos de 'cidades inteligentes' (smart cities).

A implementação do reconhecimento facial em espaços públicos tem sido justificada pela necessidade de capturar criminosos e prevenir atos de violência. No entanto, a utilização dessa tecnologia levanta graves preocupações em relação à privacidade, à proteção de dados pessoais e, sobretudo, à igualdade racial. Diversos estudos têm demonstrado que os algoritmos de reconhecimento facial apresentam taxas de erro significativamente maiores quando aplicados a pessoas negras, especialmente mulheres negras, em comparação com homens brancos.

Essa disparidade de precisão decorre, em grande parte, da falta de diversidade nos bancos de dados utilizados para treinar os algoritmos, que são predominantemente compostos por faces de pessoas brancas. Além disso, as próprias técnicas de iluminação e captura de imagem historicamente favoreceram tons de pele mais claros. No contexto do sistema de justiça criminal, os 'falsos positivos' gerados por essas falhas tecnológicas têm consequências devastadoras, resultando em abordagens policiais abusivas, prisões injustas e violações de direitos fundamentais.

No Brasil, a adoção do reconhecimento facial por governos estaduais e municipais tem avançado rapidamente, muitas vezes sem o devido debate público e sem a implementação de salvaguardas legais adequadas. Casos de prisões equivocadas baseadas em falhas do sistema já foram documentados em diversas cidades brasileiras, evidenciando como a tecnologia pode atuar como um catalisador do racismo estrutural e da seletividade penal. A presunção de infalibilidade da máquina frequentemente se sobrepõe ao depoimento do indivíduo, invertendo o ônus da prova e exigindo que o cidadão prove que não é a pessoa identificada pelo algoritmo.

A vigilância biométrica massiva transforma o espaço público em um ambiente de constante escrutínio, inibindo o exercício de liberdades fundamentais, como o direito de ir e vir, a liberdade de expressão e o direito de reunião. A captura indiscriminada de dados biométricos de milhares de transeuntes inocentes, sem o seu consentimento, viola os princípios da necessidade e da proporcionalidade, configurando uma intrusão desmedida do Estado na esfera de privacidade dos cidadãos. O efeito inibidor (chilling effect) gerado pela consciência de estar sendo constantemente monitorado compromete a vitalidade do espaço público democrático.

Diante desses riscos, diversas organizações da sociedade civil e pesquisadores têm

defendido o banimento (ban) ou a imposição de moratórias ao uso do reconhecimento facial para fins de segurança pública, até que sejam estabelecidos marcos regulatórios rigorosos e comprovada a eficácia e a equidade da tecnologia. Algumas cidades nos Estados Unidos e na Europa já aprovaram legislações restringindo ou proibindo o uso dessa ferramenta por agências policiais, reconhecendo os perigos inerentes à vigilância biométrica descontrolada.

3.4 Desafios Éticos e Jurídicos na Era Digital

A utilização de novas tecnologias como ferramentas de controle social penal impõe desafios complexos ao Direito e à ética. O descompasso entre a velocidade da inovação tecnológica e o tempo de resposta do legislador cria lacunas normativas que são frequentemente preenchidas por práticas estatais à margem do devido processo legal. A regulação dessas tecnologias exige um esforço interdisciplinar, envolvendo juristas, cientistas da computação, sociólogos e a sociedade civil como um todo.

Um dos principais desafios reside na proteção de dados pessoais no âmbito da segurança pública e da persecução penal. A Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira (Lei nº 13.709/2018) exclui de seu escopo de aplicação o tratamento de dados realizado para fins exclusivos de segurança pública, defesa nacional e atividades de investigação e repressão de infrações penais, remetendo a regulação dessa matéria a uma lei específica, que ainda não foi editada. Essa exclusão cria um vácuo jurídico preocupante, deixando o tratamento de dados sensíveis na esfera penal sujeito a normativas esparsas e insuficientes.

Essa lacuna legislativa deixa os cidadãos vulneráveis a abusos e arbitrariedades, permitindo o compartilhamento descontrolado de bases de dados entre diferentes órgãos estatais e empresas privadas, sem critérios claros de transparência, finalidade e temporalidade. A ausência de um marco legal específico para a proteção de dados na esfera penal compromete o direito à autodeterminação informativa e dificulta a responsabilização do Estado por eventuais danos causados pelo uso indevido de tecnologias de vigilância. É imperativa a aprovação de uma legislação que estabeleça princípios, direitos dos titulares e obrigações para os agentes de tratamento no âmbito da segurança pública.

Outro desafio fundamental é a garantia do devido processo legal e do direito à ampla defesa face às decisões algorítmicas. O uso de sistemas de IA para embasar decisões sobre prisões cautelares, concessão de liberdade provisória, progressão de regime ou dosimetria da pena exige que os critérios utilizados pelos algoritmos sejam transparentes, explicáveis e passíveis de contestação. O acusado tem o direito de conhecer os fundamentos que embasam uma decisão que restringe sua liberdade, não podendo o Estado se escudar no segredo comercial ou na complexidade técnica para negar esse direito. A opacidade algorítmica é incompatível com a exigência constitucional de motivação das decisões judiciais.

Ademais, é imperativo enfrentar a questão dos vieses algorítmicos e da discriminação tecnológica. O Direito Penal não pode cancelar a utilização de ferramentas que reproduzem e aprofundam desigualdades históricas. A implementação de qualquer tecnologia de controle social deve ser precedida de rigorosas avaliações de impacto sobre os direitos fundamentais, com a participação da sociedade civil e de especialistas independentes, garantindo-se a suspensão ou o banimento de sistemas que se mostrem incompatíveis com os princípios constitucionais da igualdade e da não discriminação. A auditoria algorítmica deve se tornar uma prática rotineira e obrigatória no âmbito da justiça criminal.

Por fim, faz-se necessária uma reflexão ética sobre os limites da vigilância na sociedade democrática. A busca pela segurança absoluta por meio do controle tecnológico total é uma ilusão perigosa que flerta com o autoritarismo. O Estado de Direito pressupõe a existência de espaços de opacidade e de liberdade, imunes ao escrutínio estatal. A aceitação acrítica do panóptico digital ameaça corroer as bases da cidadania e da dignidade humana, transformando os indivíduos em meros objetos de gestão algorítmica. A tecnologia deve ser um instrumento para a promoção dos direitos humanos, e não uma ferramenta para a sua supressão.

4 CONCLUSÃO

A análise empreendida neste artigo evidencia que as novas tecnologias de informação e comunicação, em especial a inteligência artificial e a análise de Big Data, têm provocado uma profunda reconfiguração nos mecanismos de controle social e na atuação do sistema de justiça criminal. A transição para um modelo de governança algorítmica instaura um 'panóptico digital', caracterizado pela vigilância ubíqua, pela predição de comportamentos e pela gestão atuarial de riscos. Essa nova racionalidade governamental desloca o foco da punição reativa para a intervenção preventiva, alterando substancialmente as bases do Direito Penal moderno.

Embora o discurso oficial legitime a adoção dessas ferramentas com base em promessas de eficiência, objetividade e modernização da segurança pública, a realidade demonstra que as tecnologias de controle social frequentemente operam como vetores de reprodução e amplificação de desigualdades estruturais. O policiamento preditivo e o reconhecimento facial, ao se alimentarem de dados enviesados e refletirem práticas discriminatórias do passado, tendem a hipervigilar e supercriminalizar populações historicamente marginalizadas, potencializando a seletividade inerente ao Direito Penal. A tecnologia, nesse contexto, atua como um mecanismo de legitimação científica do racismo estrutural e da criminalização da pobreza.

A opacidade dos sistemas algorítmicos e a ausência de marcos regulatórios adequados, especialmente no que tange à proteção de dados pessoais na esfera penal, comprometem garantias fundamentais como o devido processo legal, a presunção de inocência, a privacidade e a igualdade. A delegação de decisões que afetam a liberdade

e a dignidade humana a sistemas automatizados de 'caixa preta' representa um retrocesso civilizatório incompatível com os ditames do Estado Democrático de Direito. A impossibilidade de auditar e contestar as decisões algorítmicas esvazia o direito à ampla defesa e fragiliza o controle de legalidade sobre os atos estatais.

Diante desse cenário, conclui-se que o enfrentamento dos desafios impostos pelo controle social tecnológico exige uma postura crítica e proativa por parte da comunidade jurídica e da sociedade civil. É urgente a edição de uma legislação específica que regule o tratamento de dados para fins de segurança pública e persecução penal, preenchendo a lacuna deixada pela LGPD. Essa legislação deve estabelecer limites claros, mecanismos de transparência, auditorias independentes e responsabilização por danos, garantindo que o uso da tecnologia esteja subordinado ao respeito aos direitos fundamentais.

O Direito Penal do século XXI não pode se render ao determinismo tecnológico nem à sedução do controle absoluto. A tecnologia deve estar a serviço da emancipação humana e da promoção da justiça, e não atuar como um instrumento de opressão e exclusão. A construção de limites ético-jurídicos rigorosos ao uso de novas tecnologias é condição indispensável para preservar a essência da democracia e garantir que a sociedade da informação não se converta em uma distopia da vigilância. A defesa das garantias penais e processuais penais adquire, na era digital, uma nova e premente dimensão: a proteção do indivíduo contra o arbítrio tecnológico do Estado.

5 REFERÊNCIAS

- ANDRADE, Vera Regina Pereira de. A ilusão de segurança jurídica: do controle da violência à violência do controle penal. Porto Alegre: Livraria do Advogado, 2003.
- CASTELLS, Manuel. A sociedade em rede. São Paulo: Paz e Terra, 1999.
- DELEUZE, Gilles. Post-scriptum sobre as sociedades de controle. In: Conversações. São Paulo: Editora 34, 1992.
- FOUCAULT, Michel. Vigiar e punir: nascimento da prisão. Petrópolis: Vozes, 2014.
- GARLAND, David. A cultura do controle: crime e ordem social na sociedade contemporânea. Rio de Janeiro: Revan, 2008.
- HARCOURT, Bernard W. Against prediction: profiling, policing, and punishing in an actuarial age. Chicago: University of Chicago Press, 2007.
- O'NEIL, Cathy. Weapons of math destruction: how big data increases inequality and threatens democracy. New York: Crown, 2016.
- SILVA, Pablo Rodrigo Alflen da. Criminologia e controle social. Porto Alegre: Nuria Fabris, 2011.
- ZAFFARONI, Eugenio Raúl. Em busca das penas perdidas: a perda de legitimidade do



sistema penal. Rio de Janeiro: Revan, 1991.

ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020.