A DUPLA FACE DE JANUS: TECNOLOGIA, INOVAÇÃO E O IMPERATIVO DA GOVERNANÇA DEMOCRÁTICA EM PROJETOS DE SEGURANÇA PÚBLICA

THE TWO FACE OF JANUS: TECHNOLOGY, INNOVATION AND THE IMPERATIVE OF DEMOCRATIC GOVERNANCE IN PUBLIC SECURITY PROJECTS

Douglas Angelo Ferrari[1]

Priscila Luciene Santos de Lima[2]

Resumo: O presente artigo jurídico-científico realiza uma análise aprofundada e multifacetada sobre as complexas e, por vezes, antagônicas intersecções entre a vertiginosa adoção de tecnologias emergentes em projetos de segurança pública e a imperativa salvaguarda do arcabouço de direitos e garantias fundamentais consolidado no ordenamento jurídico brasileiro. Em face da crescente e, frequentemente, acrítica implementação de ferramentas de alta capacidade tecnológica – como sistemas de Inteligência Artificial para reconhecimento facial biométrico e policiamento preditivo, análise de Big Data, veículos aéreos não tripulados (drones) e câmeras corporais (bodycams) – emerge uma aguda tensão dialética. De um lado, a promessa de uma otimização sem precedentes da eficiência estatal na prevenção, investigação e repressão da criminalidade; de outro, a ameaça concreta de erosão de garantias constitucionais basilares, como a privacidade, a intimidade, a presunção de inocência, a isonomia e o devido processo legal. A pesquisa, de natureza qualitativa e desenvolvida por meio de método hipotético-dedutivo, com base em exaustiva revisão bibliográfica e documental, investiga os fundamentos e os limites constitucionais e legais que balizam o uso dessas tecnologias. Aprofunda-se nas intrincadas implicações jurídicas daí decorrentes, com especial enfoque na controversa aplicabilidade da Lei Geral de Proteção de Dados (LGPD) ao setor, nos desafios epistemológicos e processuais da prova algorítmica e na complexa imputação de responsabilidade por danos causados por sistemas autônomos. Ademais, o trabalho explora com densidade os aspectos éticos, sociológicos e políticos, notadamente o risco sistêmico de vieses algorítmicos discriminatórios, que perpetuam e opacificam o racismo estrutural, e o progressivo estabelecimento de uma sociedade de controle panóptico. Por fim, o artigo não se limita ao diagnóstico, mas avança para o campo propositivo, analisando e defendendo

[1] Possui graduação em Gestão Pública pelo Centro Universitário Internacional (2017), especialização em Atualização Profissional em Polícia Comunitária pelo Centro Universitário Leonardo da Vinci (2022), especialização em Direito público pela Faculdade Legale(2020), especialização em Segurança pública pela FACULDADE UNINA (2020) e especialização em Direito Penal e Processo Penal pela FACULDADE UNINA (2022). Atualmente é Policial Militar da Policia Militar do Paraná. Lattes: http://lattes.cnpq.br/6162042230506144.

[2] Pós-doutora em Novas Tecnologias e Direito pela Università Mediterranea di Reggio Calabria - ITÁLIA. Realizando estágio Pós-doutoral no Programa de Pós-Graduação em Ciências Jurídicas da Universidade Federal da Paraíba (UFPB). Doutora em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie (MACKENZIE). Mestre em Direito Empresarial e Cidadania pelo Centro Universitário Curitiba (UNICURITIBA). Diretora Editorial e Conselheira de inúmeros periódicos científicos, nacionais e internacionais. Associada e Integrante do Cadastro Nacional e Internacional de Avaliadores do Conselho Nacional de Pesquisa e Pós-graduação em Direito (CONPEDI). Email: pritysantoslima@hotmail.com. Lattes: http://lattes.cnpq.br/7325012453913306

a construção de modelos de governança tecnológica como único caminho para a harmonização do binômio segurança-liberdade. Sustenta-se que a legitimidade de tais inovações depende da edificação de um ecossistema regulatório robusto, fundado nos pilares da transparência radical, da accountability efetiva, da equidade algorítmica e do controle social-democrático.

Palavras-chave: Segurança Pública. Tecnologia. Direitos Fundamentais. Governança Algorítmica. Proteção de Dados.

Abstract: This scientific-legal article conducts an in-depth, multifaceted analysis of the complex and often antagonistic intersections between the vertiginous adoption of emerging technologies in public security projects and the imperative safeguarding of the fundamental rights and guarantees framework consolidated in the Brazilian legal system. Faced with the growing and frequently uncritical implementation of high-tech tools—such as Artificial Intelligence systems for biometric facial recognition and predictive policing, Big Data analytics, unmanned aerial vehicles (drones), and body-worn cameras (bodycams)—an acute dialectical tension emerges. On one hand, the promise of an unprecedented optimization of state efficiency in crime prevention, investigation, and repression; on the other, the concrete threat of erosion of basic constitutional guarantees, such as privacy, intimacy, the presumption of innocence, equality, and due process. The research, qualitative in nature and developed through a hypothetical-deductive method based on an exhaustive bibliographic and documentary review, investigates the constitutional and legal foundations and limits that guide the use of these technologies. It delves into the intricate legal implications arising therefrom, with a special focus on the controversial applicability of the General Data Protection Law (LGPD) to the sector, the epistemological and procedural challenges of algorithmic evidence, and the complex attribution of liability for damages caused by autonomous systems. Furthermore, the work densely explores the ethical, sociological, and political aspects, notably the systemic risk of discriminatory algorithmic biases that perpetuate and obscure structural racism, and the progressive establishment of a panoptic control society. Finally, the article is not limited to diagnosis but advances into the propositional field, analyzing and advocating for the construction of technological governance models as the only path to harmonize the security-liberty binomial. It is argued that the legitimacy of such innovations depends on the establishment of a robust regulatory ecosystem, founded on the pillars of radical transparency, effective accountability, algorithmic fairness, and democratic social control.

Keywords: Public Security. Technology. Fundamental Rights. Algorithmic Governance. Data Protection.

1. INTRODUÇÃO

A segurança pública, alçada pela Constituição da República Federativa do Brasil de 1988 (CRFB/88) à condição de direito fundamental e dever irrenunciável do Estado, encontra-se no epicentro de uma transformação paradigmática impulsionada pela chamada Quarta Revolução Industrial. Este novo cenário, caracterizado pela fusão de tecnologias e pela indistinção entre os mundos físico, digital e biológico, introduz um arsenal de inovações que prometem redefinir radicalmente as estratégias

de prevenção, investigação e repressão criminal. Ferramentas baseadas em Inteligência Artificial (IA), a capacidade de processamento de volumes massivos e heterogêneos de dados (*Big Data*), o monitoramento ubíquo por veículos aéreos não tripulados (drones) e câmeras corporais, e a identificação biométrica em larga escala são crescentemente integrados aos projetos de segurança, acenando com uma promessa de eficiência e preditividade sem precedentes.

Essa transição tecnológica, contudo, é marcadamente ambivalente. Se por um lado oferece novas e poderosas capacidades de vigilância e controle, por outro, potencializa ameaças de magnitude inédita aos direitos e garantias fundamentais. A implementação açodada e desprovida de rigorosas balizas normativas e éticas pode erodir o núcleo essencial da privacidade, da intimidade, da presunção de inocência, da não discriminação e do devido processo legal. Mais do que isso, arrisca-se a instituir um estado de vigilância permanente, uma transição do "panóptico" disciplinar de Foucault para um "panóptico digital", onde o poder se torna mais difuso, automatizado e invisível, conformando o que Gilles Deleuze (1992) anteviu como as "sociedades de controle", cujo poder é exercido não mais pelo confinamento, mas por uma modulação contínua do comportamento em rede. A questão transcende o mero aparato técnico, pois, como adverte David Lyon (2009, p. 15), "a vigilância é muito mais do que a simples observação, pois está tipicamente associada à administração, à governança, à influência e à proteção". A vigilância algorítmica, portanto, não é um mero ato de ver, mas um ato de governar, de classificar e de intervir na vida dos cidadãos, muitas vezes de forma preemptiva e opaca.

Nesse contexto de alta complexidade, emerge o problema de pesquisa central deste trabalho: De que forma a implementação de tecnologias inovadoras em projetos de segurança pública no Brasil pode ser juridicamente conformada e democraticamente governada para que, ao invés de antagonizar, harmonize a busca por eficiência estatal com a proteção dos direitos fundamentais e os preceitos da Lei Geral de Proteção de Dados (LGPD), garantindo uma governança ética, equitativa e transparente?

A relevância jurídica e social do tema é superlativa. De um lado, a sociedade, premida por elevados índices de violência, clama por respostas mais eficazes do Estado. De outro, a comunidade jurídica, a academia e a sociedade civil organizada alertam para os perigos de uma distopia tecnológica, onde a busca por segurança resulte no sacrifício de liberdades duramente conquistadas e na opacificação de um

"Estado de Direito Algorítmico", no qual a lei e o devido processo são substituídos por decisões automatizadas inescrutáveis.

O objetivo geral deste artigo é, portanto, analisar a complexa e tensa relação entre inovação tecnológica na segurança pública e o regime de proteção de direitos fundamentais, propondo balizas teóricas e práticas para sua coexistência harmônica. Os objetivos específicos são: a) dissecar os fundamentos e limites constitucionais para o uso de tecnologia na segurança pública, com ênfase na aplicação do princípio da proporcionalidade; b) detalhar o funcionamento técnico das principais tecnologias emergentes, expondo suas potencialidades e seus riscos intrínsecos; c) realizar uma análise crítica das implicações jurídicas e dos desafios regulatórios; d) aprofundar a discussão sobre os dilemas éticos e sociais, com destaque para o fenômeno do viés algorítmico; e e) delinear modelos de governança para uma implementação responsável e controlada.

A metodologia empregada consiste na pesquisa bibliográfica e documental, de natureza qualitativa e com a utilização do método de abordagem hipotético-dedutivo. A análise partirá do arcabouço normativo geral para as questões específicas e aplicadas, fundamentando-se em doutrina especializada multidisciplinar, abrangendo o Direito, a Ciência da Computação, a Sociologia e a Ética, bem como na análise crítica de legislação, projetos de lei e jurisprudência nacional e comparada.

2. FUNDAMENTOS E LIMITES NORMATIVOS: O CAMPO DE TENSÃO CONSTITUCIONAL

A atuação do Estado no âmbito da segurança pública não ocorre em um espaço de discricionariedade ilimitada. Ela é rigorosamente balizada por um complexo de normas e princípios que formam um campo de permanente tensão dialética.

De um lado, o art. 144 da CRFB/88 estabelece a segurança como dever do Estado. De outro, toda e qualquer ação estatal encontra limites intransponíveis nos direitos e garantias fundamentais. A CRFB/88 não admite hierarquias apriorísticas que submetam a liberdade à segurança. Vigora o princípio da "unidade da Constituição", que impõe a interpretação do texto constitucional de forma a evitar contradições (SARLET, 2015, p. 321). Assim, o direito à segurança não pode aniquilar o núcleo essencial de outros direitos, como a intimidade (art. 5º, X), a proteção de dados (EC 115/2022) e a presunção de inocência (art. 5º, LVII). Como ensina Konrad Hesse (1991, p. 57) sobre a força normativa da Constituição, a norma constitucional não pode

ser reduzida a uma mera folha de papel; ela pretende ser convertida na realidade, vinculando o poder estatal. A Emenda Constitucional nº 115/2022, ao elevar a proteção de dados pessoais à categoria de direito fundamental autônomo, reforçou de maneira inequívoca essa barreira, exigindo que qualquer tratamento de dados pelo Estado, mesmo para fins de segurança, seja estritamente justificado e limitado.

A única via legítima para a harmonização desse conflito reside na aplicação criteriosa do princípio da proporcionalidade. Conforme leciona Luís Roberto Barroso (2020, p. 245), a proporcionalidade é "um princípio instrumental e uma regra de interpretação para a solução de conflitos entre princípios constitucionais", exigindo um exame de adequação, necessidade e ponderação.

Adequação (ou Idoneidade): A medida tecnológica deve ser empiricamente apta a fomentar o objetivo almejado. Não basta a mera promessa de eficácia; é preciso demonstrar, com dados auditáveis, que a tecnologia efetivamente contribui para a redução da criminalidade de forma significativa.

Necessidade (ou Proibição do Excesso): A medida deve ser a menos gravosa aos direitos fundamentais dentre todas as alternativas igualmente eficazes. Este exame impõe ao Estado um ônus argumentativo pesado: provar que não existem outros meios – tecnológicos ou não – que possam atingir o mesmo nível de eficácia com menor intrusão na esfera privada dos cidadãos.

Proporcionalidade em sentido estrito: Trata-se do sopesamento final. Como aduz Virgílio Afonso da Silva (2010, p. 182), a proporcionalidade "não é uma fórmula matemática, mas um método argumentativo que exige justificação pública e racional para as restrições de direitos". Neste ponto, a "Fórmula do Peso" de Robert Alexy (2017) oferece um modelo analítico, embora não mecânico, ao postular que "quanto maior for o grau de não satisfação ou de afetação de um princípio, tanto maior terá que ser a importância da satisfação do outro". Aplicada ao nosso caso, a intensidade da violação da privacidade pela vigilância massiva deve ser justificada por um ganho concreto e de altíssima importância para a segurança coletiva, o que raramente é demonstrado na prática.

Portanto, a simples alegação genérica de "combate à criminalidade" é manifestamente insuficiente. É imperativo demonstrar, para cada projeto, que sua implementação sobrevive a esse rigoroso escrutínio.

3. O ARSENAL TECNOLÓGICO: ANATOMIA DAS FERRAMENTAS E RISCOS INTRÍNSECOS

A compreensão das implicações jurídicas pressupõe um conhecimento mínimo do funcionamento das tecnologias.

3.1 Inteligência artificial (IA): o poder e o perigo da automação cognitiva

Sistemas de Reconhecimento Facial Biométrico: Estes sistemas comparam um rosto capturado com um vasto banco de dados (identificação 1:N). O risco de erros e vieses é documentado. Relatórios do *National Institute of Standards and Technology* (NIST) dos EUA têm consistentemente apontado que "sistemas de reconhecimento facial podem produzir resultados demograficamente diferenciais", com taxas de falsos positivos (identificações incorretas) significativamente mais altas para mulheres negras e asiáticas, e também para os muito jovens e os muito idosos, em comparação com homens brancos de meia-idade (NIST, 2019). Um falso positivo no contexto da segurança pública não é um mero inconveniente; pode levar a uma abordagem policial equivocada, a uma prisão indevida e a um trauma indelével.

Análise Preditiva de Crimes (Policiamento Preditivo): Utiliza algoritmos para prever locais ou pessoas com maior propensão à criminalidade. O risco reside no "ciclo de retroalimentação discriminatório": dados históricos enviesados (que refletem a prática policial, não a criminalidade real) alimentam o algoritmo, que por sua vez direciona a polícia para as mesmas áreas, confirmando o viés inicial. Por exemplo, se uma área com população predominantemente negra é historicamente mais policiada, mais crimes de menor potencial ofensivo (como posse de drogas para consumo) serão registrados ali. O algoritmo, "aprendendo" com esses dados, rotulará a área como um "*hotspot*", levando a ainda mais policiamento e prisões, o que "prova" que o algoritmo estava certo, criando uma profecia autorrealizável que mascara e aprofunda a discriminação racial.

3.2 Câmeras corporais (*bodycams*): a tecnologia da dupla vigilância

As *bodycams* são apresentadas como solução para aumentar a transparência policial. Contudo, elas transformam cada policial em um sensor móvel de coleta de dados. A regulamentação sobre quando gravar, quem acessa as imagens e como são utilizadas é crucial e não pode ser deixada à discricionariedade de cada corporação. O debate internacional abrange questões como a gravação contínua versus a

gravação acionada pelo policial (que dá ao agente o poder de decidir o que será "história oficial"), as políticas de retenção de dados (armazenar tudo indefinidamente cria um vasto repositório para vigilância futura) e o uso de softwares de análise facial sobre as imagens coletadas, o que transformaria uma ferramenta de *accountability* em mais um instrumento de vigilância em massa.

3.3 *Blockchain* e a busca pela integridade da prova digital

Em contraponto, o *blockchain* surge com potencial para o fortalecimento de garantias processuais. Sua arquitetura de registro distribuído e imutável pode ser aplicada para criar uma cadeia de custódia digital robusta, garantindo a integridade da prova desde sua coleta até sua apresentação em juízo. Por exemplo, o *hash* (assinatura digital única) de um vídeo gravado por uma câmera corporal poderia ser imediatamente registrado em um *blockchain*, tornando qualquer alteração posterior no arquivo facilmente detectável e documentando de forma inviolável cada acesso ou análise daquela evidência.

4. IMPLICAÇÕES JURÍDICAS: A CRISE DOS PARADIGMAS TRADICIONAIS

A inserção dessas tecnologias no sistema de justiça criminal coloca em xeque conceitos jurídicos tradicionais.

4.1 A Lei Geral de Proteção de Dados e o limbo da "LGPD Penal"

A LGPD (Lei nº 13.709/2018) excepciona sua aplicação para fins de segurança pública (art. 4º, III), remetendo a matéria a uma "legislação específica". Na ausência dessa lei, instala-se um perigoso limbo jurídico. Contudo, a doutrina é firme ao afirmar que a exceção não é um "cheque em branco". Para Danilo Doneda (2019, p. 125), os princípios da LGPD, por derivarem da Constituição, devem ser aplicados por analogia. Marcel Leonardi (2019, p. 88) reforça que "a ausência de uma lei específica não significa a existência de uma terra sem lei", devendo-se observar os princípios constitucionais. O modelo da Diretiva (UE) 2016/680 (*Law Enforcement Directive*) da União Europeia serve de paradigma, ao estabelecer um regime de proteção de dados específico para a área penal, com regras claras sobre finalidade, limitação, exatidão, prazos de conservação e direitos dos titulares, demonstrando que eficiência investigativa e proteção de dados não são mutuamente excludentes.

4.2 A prova algorítmica e a crise da epistemologia processual

Como valorar uma prova gerada por um algoritmo? A jurisprudência do STJ, notadamente no Habeas Corpus nº 598.886/SC, oferece um norte crucial: o reconhecimento, seja humano ou algorítmico, não pode ser prova absoluta, mas um mero ato investigativo que demanda corroboração por provas independentes. A opacidade de muitos algoritmos (*black box*) viola o direito à ampla defesa. Frank Pasquale define a questão de forma contundente:

> A sociedade da caixa-preta é um estado de jogo em que as instituições e empresas poderosas tomam decisões cada vez mais importantes com base em modelos secretos e impenetráveis. [...] A falta de transparência sobre como esses sistemas funcionam pode levar a erros, preconceitos e uma erosão da responsabilidade democrática. (PASQUALE, 2015, p. 3, tradução nossa).

Para Aury Lopes Jr. (2020, p. 345), no processo penal, "a prova tem uma finalidade retrospectiva, de reconstruir um fato passado", e se os critérios dessa reconstrução são opacos, a própria noção de prova é comprometida. Surge a necessidade de um "devido processo legal algorítmico", que garanta não apenas a ciência da decisão automatizada, mas o direito a uma explicação significativa sobre sua lógica e o direito de contestá-la eficazmente perante um revisor humano com poder de decisão.

4.3 Responsabilidade civil e penal: o desafio da imputação na era da IA

Se um erro de um sistema de IA causa um dano, a quem imputar a responsabilidade? A responsabilidade objetiva do Estado (art. 37, § 6º, da CRFB/88) é um ponto de partida, mas pode ser insuficiente. É preciso discutir a responsabilidade do desenvolvedor, do agente público que confiou acriticamente na tecnologia e do gestor que a implementou. A complexidade dos sistemas de IA desafia a dogmática tradicional do nexo de causalidade, podendo exigir a adoção de regimes de responsabilidade distribuída ou solidária entre os diversos atores da cadeia produtiva e de uso da tecnologia, além de seguros obrigatórios para atividades de alto risco.

5. ASPECTOS ÉTICOS E SOCIAIS: A DIMENSÃO OCULTA DA VIGILÂNCIA

5.1 Viés algorítmico e a codificação da discriminação

Este é o mais insidioso dos perigos. Os algoritmos aprendem com dados que refletem uma sociedade desigual, resultando na criação de "armas de destruição matemática" (O'NEIL, 2016). Shoshana Zuboff oferece uma definição precisa do motor por trás desse fenômeno:

> O capitalismo de vigilância reivindica unilateralmente a experiência humana como matéria-prima gratuita para tradução em dados comportamentais. [...] Esses dados são declarados como um excedente comportamental proprietário, alimentados em processos de fabricação avançados conhecidos como 'inteligência de máquina', e fabricados em produtos de previsão que antecipam o que você fará agora, em breve e mais tarde. (ZUBOFF, 2019, p. 8, tradução nossa).

No contexto da segurança pública, o "produto de previsão" é a probabilidade de um indivíduo cometer um crime, e a "matéria-prima" são dados que já carregam os vieses de uma sociedade estruturalmente racista. Ruha Benjamin (2019, p. 9) vai além, cunhando o termo "O Novo Código Jim Crow" e afirmando que "a automação não elimina o viés, mas o camufla com o verniz da objetividade técnica". Similarmente, Safiya Umoja Noble (2018) demonstra em "*Algorithms of Oppression*" como os resultados de buscas na internet podem perpetuar estereótipos negativos. O resultado é a perpetuação do que Silvio Almeida (2019) define como racismo estrutural, agora codificado em software e operando com uma velocidade e escala sem precedentes.

5.2 O "*chilling effect*" e a arquitetura do controle

A consciência de uma vigilância onipresente gera um "efeito inibidor" (*chilling effect)* sobre o exercício das liberdades. O medo de ser mal interpretado por um algoritmo pode levar à autocensura e à retração do espaço cívico. Aqui, a tese de Lawrence Lessig é fundamental. Ele argumenta que o comportamento online não é regulado apenas pela lei, mas por quatro forças: lei, normas sociais, mercado e arquitetura (ou código). Sobre esta última, ele afirma

> O código, ou a arquitetura do ciberespaço, é uma forma de regulação. Ele estabelece os termos sob os quais a vida no ciberespaço é vivida. É a "física" do mundo virtual. [...] A arquitetura pode restringir a liberdade de maneiras que a lei não pode, e pode fazê-lo de forma mais eficaz. (LESSIG, 2006, p. 125, tradução nossa).

Um sistema de vigilância onipresente é uma arquitetura que regula o comportamento social pelo medo. Por exemplo, a instalação massiva de câmeras com reconhecimento facial em uma praça pública pode inibir a realização de protestos políticos, a organização de reuniões comunitárias ou mesmo a simples permanência de populações em situação de rua, que passam a ser vistas como "anomalias" a serem monitoradas e removidas pelo sistema, independentemente de qualquer sanção legal explícita.

6. MODELOS DE GOVERNANÇA: PARA UMA INOVAÇÃO RESPONSÁVEL E DEMOCRÁTICA

A solução não está na tecnofobia, mas na governança democrática da tecnologia.

Marco Regulatório Específico e Protetivo: É urgente a edição da "LGPD Penal" e de uma lei geral sobre IA (a exemplo do PL 2338/2023). Tal marco deve proibir práticas de risco inaceitável (e.g., *social scoring*, policiamento preditivo sobre pessoas), estabelecer moratórias para tecnologias de alto risco ainda imaturas (como o reconhecimento facial em tempo real em espaços públicos) e exigir supervisão humana qualificada, efetiva e significativa.

Avaliação Prévia e Periódica de Impacto Algorítmico (AIA): Nenhuma tecnologia de alto risco deve ser implementada sem uma rigorosa Avaliação de Impacto nos Direitos Fundamentais, com participação social e resultados públicos. Essa avaliação deve analisar não apenas a precisão técnica, mas também o potencial de impacto discriminatório e os riscos para as liberdades civis.

Transparência Radical e Auditabilidade (Explainable AI - XAI): O princípio da publicidade deve ser a regra. Os cidadãos afetados por decisões automatizadas devem ter o direito a uma explicação compreensível, um princípio defendido por Luciano Floridi (2018) como essencial para a ética da IA. Isso implica a obrigação de documentação clara dos sistemas, a possibilidade de auditoria por órgãos de controle e pela sociedade civil, e a criação de registros públicos de quais tecnologias de vigilância estão em uso, onde e com qual finalidade.

Controle Social e Institucional: A decisão sobre quais tecnologias adotar é política. É preciso criar mecanismos de controle, como audiências públicas vinculantes, a criação de conselhos de ética com participação da sociedade civil e da academia, e fiscalização rigorosa pelo Ministério Público e Defensoria Pública. A

criação de "sandboxes regulatórios" controlados, onde novas tecnologias podem ser testadas em ambiente limitado e sob supervisão estrita antes de uma possível implementação em larga escala, também se mostra uma ferramenta prudente.

7. CONCLUSÃO

A tecnologia, em sua essência, é ambivalente; pode tanto libertar quanto oprimir. A direção que ela tomará no campo da segurança pública brasileira não é um destino pré-determinado, mas uma escolha política e jurídica que estamos fazendo no presente, em cada licitação, em cada projeto de lei, em cada decisão judicial.

Este artigo demonstrou que a incorporação de inovações tecnológicas na segurança pública é um fenômeno de altíssima complexidade, que tensiona os pilares do Estado Democrático de Direito e desafia conceitos jurídicos consolidados. A harmonização entre eficiência tecnológica e proteção de direitos é a única condição de legitimidade para tais projetos, e ela exige ser construída ativamente por meio de um ecossistema de governança democrática, robusto e vigilante. Essa governança não pode ser um mero acessório, mas o núcleo central da estratégia de inovação.

Tal governança requer a superação do perigoso vácuo legislativo, a imposição de deveres de transparência, equidade e *accountability* ao poder público e aos seus fornecedores privados, a submissão intransigente de toda e qualquer medida ao crivo da proporcionalidade e a garantia de um controle humano significativo e de uma supervisão social e institucional efetiva. Ignorar esses imperativos em nome de uma promessa tecnocrática e falaciosa de segurança absoluta é um caminho que leva, invariavelmente, à erosão da liberdade e à consolidação de formas de controle autoritário. A verdadeira segurança, em uma democracia constitucional, não se mede apenas pela ausência de crime, mas, fundamentalmente, pela presença vibrante da liberdade e pela garantia da dignidade de todas as pessoas, sem discriminação.

REFERÊNCIAS

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Tradução de Virgílio Afonso da Silva. 2. ed. São Paulo: Malheiros, 2017.

ALMEIDA, Silvio Luiz de. **Racismo Estrutural**. São Paulo: Sueli Carneiro; Pólen, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 6023**: Informação e documentação – Referências – Elaboração. Rio de Janeiro, 2018.

BADARÓ, Gustavo Henrique. **Epistemologia Judiciária e Prova Penal**. São Paulo: Thomson Reuters Brasil, 2020.

BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo**: os conceitos fundamentais e a construção do novo modelo. 9. ed. São Paulo: Saraiva, 2020.

BAUMAN, Zygmunt. **Modernidade Líquida**. Tradução de Plínio Dentzien. Rio de Janeiro: Jorge Zahar Editor, 2001.

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

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: <https://www.planalto.gov.br/ccivil_03/-constituicao/constituicao.htm>. Acesso em: 6 jun. 2025.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir no rol dos direitos e garantias fundamentais o da proteção de dados pessoais, inclusive nos meios digitais. Brasília, DF: Presidência da República. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/-emendas/emc/emc115.htm>. Acesso em: 6 jun. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 6 jun. 2025.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Brasília, DF: Presidência da República. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm>. Acesso em: 6 jun. 2025.

BRASIL. Superior Tribunal de Justiça. **Habeas Corpus nº 598.886/SC**. Relator: Ministro Rogerio Schietti Cruz. Sexta Turma, julgado em 27 out. 2020, DJe 18 nov. 2020.

DELEUZE, Gilles. Post-scriptum sobre as sociedades de controle. *In*: DELEUZE, Gilles. **Conversações: 1972-1990**. Tradução de Peter Pál Pelbart. São Paulo: Editora 34, 1992. p. 219-226.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. São Paulo: Thomson Reuters Brasil, 2019.

FLORIDI, Luciano. **The Logic of Information**: A Theory of Philosophy as Conceptual Design. Oxford: Oxford University Press, 2018.

HESSE, Konrad. **A força normativa da constituição**. Tradução de Gilmar Ferreira Mendes. Porto Alegre: Sergio Antonio Fabris Editor, 1991.

LEONARDI, Marcel. **Fundamentos de direito digital**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

LESSIG, Lawrence. **Code**: Version 2.0. New York: Basic Books, 2006.

LOPES JR., Aury. **Direito processual penal**. 17. ed. São Paulo: Saraiva, 2020.

LYON, David. **Surveillance Studies**: An Overview. Cambridge: Polity Press, 2009.

MENDES, Laura Schertel; BIONI, Bruno. Proteção de dados para segurança pública: os próximos passos da LGPD. **JOTA**, Brasília, 10 ago. 2020. Opinião & Análise. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/protecao-de-dados-para-seguranca-publica-os-proximos-passos-da-lgpd-10082020>. Acesso em: 6 jun. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects**. Gaithersburg, MD: U.S. Department of Commerce, 2019. (NISTIR 8280). Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>. Acesso em: 6 jun. 2025.

NOBLE, Safiya Umoja. **Algorithms of Oppression**: How Search Engines Reinforce Racism. New York: New York University Press, 2018.

O'NEIL, Cathy. **Weapons of Math Destruction**: How Big Data Increases Inequality and Threatens Democracy. New York: Crown, 2016.

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

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2012.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 12. ed. Porto Alegre: Livraria do Advogado, 2015.

SARMENTO, Daniel. **Direito constitucional**: teoria, história e métodos de trabalho. 2. ed. Belo Horizonte: Fórum, 2016.

SILVA, Virgílio Afonso da. **Direitos fundamentais**: conteúdo essencial, restrições e eficácia. 2. ed. São Paulo: Malheiros, 2010.

UNIÃO EUROPEIA. Parlamento Europeu e Conselho. **Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados. Jornal Oficial da União Europeia, L 119, 4 maio 2016.

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