

O papel da tecnologia e da inteligência artificial na segurança pública: desafios e convergências com os direitos fundamentais individuais e sociais

The role of technology and artificial intelligence in public safety: challenges and convergences with individual and social fundamental rights

Flávio Maria Leite Pinheiro*

Sumário

1. Introdução. 2. Perspectivas sobre o estado e os direitos fundamentais em face das tecnologias digitais. 3. Breves considerações sobre direito fundamental à segurança pública e reflexões contemporâneas. 4. Novas tecnologias, inteligência artificial e segurança pública: limites e desafios. 5. Conclusões. Referências.

Resumo

A utilização de tecnologias baseadas em inteligência artificial tem um papel central na segurança pública contemporânea. A Constituição de 1988 reconhece a segurança como um dever estatal e um direito universal, embora sua implementação enfrente diversos desafios. Este artigo examina as políticas públicas de segurança na Era Digital, destacando o uso de tecnologias e sua relação com os direitos fundamentais. O problema de pesquisa levantado é: como deve ser estruturada a política de segurança pública no Brasil diante da incorporação de tecnologias e inteligência artificial, em confronto com os direitos fundamentais individuais? O método adotado é o dialético, com uma abordagem monográfica. O estudo explora os princípios contemporâneos do direito à segurança, as bases das políticas públicas e os contrastes com os direitos fundamentais. Ao final, conclui-se que o Brasil ainda não possui mecanismos eficazes para proteger os direitos individuais frente ao uso de tecnologias na segurança pública.

Abstract

The use of technologies based on artificial intelligence plays a central role in contemporary public security. The 1988 Constitution recognizes security as a state duty and a universal right, although its implementation faces several challenges. This article examines public security policies

* Pós-Doutor, Doutor e Mestre em Direito pela Universidade Federal de Santa Catarina (UFSC). Mestre em Filosofia pela Universidade Estadual do Ceará (UECE). Bacharel em Direito e Filosofia. Revisor de estudo de caso e perito do Observatório Interamericano de Governança e Inovação Pública (OIGIP), pertencente à Escola de Governo da Organização dos Estados Americanos (OEA). Membro da Rede de Especialistas da Fundação José Ortega y Gasset-Gregorio Marañón (FOM), Madrid/Espanha. Professor Adjunto na Universidade Estadual Vale do Acaraú (UVA), Sobral/CE, lotado nos cursos de Direito (graduação) e Filosofia (Mestrado). Líder do Grupo de Estudos e Pesquisas em Filosofia e Teoria Política e Social, registrado no Diretório de Grupos de Pesquisa do CNPq

in the Digital Age, highlighting the use of technologies and their relationship with fundamental rights. The research problem raised is: how should public security policy in Brazil be structured in view of the incorporation of technologies and artificial intelligence, in conflict with individual fundamental rights? The method adopted is dialectical, with a monographic approach. The study explores the contemporary principles of the right to security, the bases of public policies and the contrasts with fundamental rights. In the end, it is concluded that Brazil still does not have effective mechanisms to protect individual rights against the use of technologies in public security.

Palavras-chave: Inteligência artificial. Segurança pública. Direitos fundamentais. Políticas públicas. Reconhecimento facial.

Keywords: Artificial intelligence. Public security. Fundamental rights. Public Policies. Facial recognition.

1. Introdução

As políticas públicas desempenham um papel essencial na concretização dos direitos fundamentais, especialmente no que tange à segurança pública, um tema de grande relevância no Brasil. A Constituição Federal de 1988 consagra a segurança como um dever do Estado e um direito de todos os cidadãos, mas a implementação eficaz desse direito enfrenta diversos desafios. Um dos mais complexos diz respeito ao uso crescente de tecnologias digitais e ferramentas de inteligência artificial, como o reconhecimento facial, que vêm sendo incorporadas às práticas de segurança pública, mas ainda carecem de uma regulamentação jurídica adequada. Nesse contexto, surgem questionamentos sobre a compatibilidade dessas inovações tecnológicas com os direitos fundamentais individuais, como a privacidade e a proteção de dados.

O presente artigo tem como objetivo principal investigar a estruturação necessária das políticas de segurança pública no Brasil à luz do uso de tecnologias emergentes, especialmente a inteligência artificial, e suas implicações para os direitos fundamentais. A pesquisa busca responder à seguinte questão: como a política de segurança pública brasileira pode ser reformulada para integrar o uso de tecnologias avançadas sem violar os direitos individuais garantidos pela Constituição? A análise se propõe a explorar as interseções entre direitos fundamentais sociais e individuais, refletindo sobre a necessidade de adaptação das políticas públicas às novas demandas tecnológicas e sociais.

A metodologia utilizada é o método dialético, que permite a contraposição de diferentes pontos de vista sobre a questão, com uma abordagem monográfica focada no contexto brasileiro. Inicialmente, o estudo aborda os fundamentos teóricos do Estado em relação às novas tecnologias, analisando como autores como Manuel Castells e Pierre Lévy discutem o impacto da revolução digital nas instituições sociais e nos direitos. Castells, em sua obra sobre a "Sociedade em Rede", retrata o fenômeno da interconexão global, que alterou profundamente as relações entre Estado e sociedade, ampliando o alcance e o poder das tecnologias digitais, inclusive nas políticas de segurança pública. Lévy, por sua vez, explora o conceito de cibercultura e a transformação das práticas sociais e estatais no ciberespaço, enfatizando o papel central que a Internet e suas tecnologias desempenham na vida contemporânea. Tais autores são fundamentais para embasar a análise do impacto das tecnologias na redefinição dos direitos fundamentais e da atuação estatal.

No âmbito jurídico, o artigo examina as novas demandas que surgem com a introdução de tecnologias como a inteligência artificial, destacando a necessidade urgente de regulamentação, especialmente no que se refere à proteção dos dados pessoais e à prevenção de abusos no uso dessas ferramentas. A ausência de uma legislação específica que regule o uso de tecnologias de vigilância, como o reconhecimento facial, no contexto da segurança pública é uma lacuna crítica no arcabouço normativo brasileiro. Como apontado por autores como Ingo Sarlet e Danilo Doneda, a proteção dos dados pessoais é um dos desafios mais prementes da era digital, uma vez que o uso de grandes bases de dados e algoritmos para traçar perfis e monitorar comportamentos pode comprometer direitos fundamentais, como a privacidade e a autodeterminação informativa.

O artigo também discute o papel da inteligência artificial na segurança pública, refletindo sobre os desafios éticos e legais que seu uso impõe. A discriminação algorítmica é um dos pontos críticos, uma vez que sistemas de IA, ao processarem grandes volumes de dados, podem reforçar preconceitos e desigualdades, como já observado em outras partes do mundo. No Brasil, o uso de sistemas de reconhecimento facial para identificar suspeitos em vias públicas, por exemplo, levanta questões sobre a proteção dos direitos individuais e o risco de erros e abusos por parte das autoridades. A ausência de regulamentação adequada para o uso dessas tecnologias, conforme observam Sarlet e outros estudiosos, torna-se ainda mais preocupante diante do potencial de impacto nas liberdades civis e nos direitos humanos.

Ao longo do estudo, são discutidos os desafios práticos e teóricos envolvidos na harmonização entre segurança pública e direitos individuais em um contexto de avanços tecnológicos. A crescente adoção de tecnologias na segurança pública apresenta oportunidades para aprimorar a eficácia das políticas estatais, mas, ao mesmo tempo, exige um marco regulatório robusto que proteja os cidadãos de abusos. A análise enfatiza que, sem uma regulamentação clara, o uso de tecnologias como a inteligência artificial na segurança pública pode violar direitos fundamentais, criando um ambiente de vigilância excessiva e restrição de liberdades.

O estudo conclui que o Brasil precisa urgentemente de instrumentos jurídicos e regulatórios mais eficazes para proteger os direitos individuais diante do uso de tecnologias de segurança pública. Embora as inovações tecnológicas ofereçam soluções promissoras para enfrentar desafios contemporâneos, como o aumento da criminalidade, elas também trazem novos riscos que não podem ser ignorados. É necessário desenvolver diretrizes que equilibrem o uso dessas ferramentas com a proteção dos direitos fundamentais, garantindo que o avanço tecnológico esteja sempre a serviço da justiça social e do respeito aos direitos humanos. Assim, o artigo propõe a formulação de políticas públicas que integrem a tecnologia de maneira responsável, respeitando os princípios constitucionais e promovendo uma segurança pública que não sacrifique os direitos individuais em nome da eficiência estatal.

2. Perspectivas sobre o estado e os direitos fundamentais em face das tecnologias digitais

As novas tecnologias impulsionaram mudanças nas instituições e nos direitos, especialmente nos direitos fundamentais. Desde o surgimento da Internet, a ascensão de novos mecanismos, tecnologias, mercados e serviços vem sendo objeto de debate transversal nas mais diversas disciplinas. Diferentes movimentos teóricos tentam traçar concepções e explicações em tal sentido. Manuel Castells (2016) retrata o crescimento exponencial daquilo

que nominou como Sociedade em Rede, ou seja, relações conectadas em uma ampla rede baseada na comunicação entre todos. Essa perspectiva perpassou para a relação estatal, uma vez que a Internet se transformou em um ambiente desterritorializado e descentralizado (Castells, 2003), ampliando o debate da tutela na esfera jurídica.

Por sua vez, outro autor que busca apresentar perspectivas sobre o fenômeno digital – essencialmente pautado na Internet – é Pierre Lévy (2010) a interconexão em escala mundial de computadores é nominada como ciberespaço, no qual ocorre a cibercultura, ou seja, práticas que envolvem o crescimento do ciberespaço.

Todo esse fenômeno, erigido a partir da escala de modificação tecnológica e transmissão de informações alterou profundamente as relações sociais e estatais (Castells, 2016). A ampliação das possibilidades técnicas permite hoje que o Estado se utilize da Internet e exerça suas atividades baseadas em grandes plataformas digitais, bastando ver a recente aprovação da Lei do Governo Digital, no Brasil, e todos os impactos vindouros.

Nesse sentido, alteraram-se as perspectivas estatais e societais, fazendo-se com que os direitos fundamentais também fossem atingidos e modificados pelas novas tecnologias, iniciadas pela Internet. Landa (2016, p. 2) aponta que *“en esta nueva etapa de transformación del Estado y la sociedad, el Internet es el fundamento principal para construir la nueva identidad de los derechos fundamentales”*.

Não apenas surgiram novos direitos fundamentais, conforme Sarlet (2010), com perspectivas de direitos fundamentais de quarta ou quinta dimensão, a partir da escala que a Internet e suas tecnologias alcançaram, mas as novas relações estão a fazer com que a própria teoria dos direitos fundamentais confira uma nova identidade aos direitos fundamentais. Landa (2019) ainda aponta que a Internet não apenas transformou a equação entre os direitos, mas também se tornou ela um direito fundamental quando permitiu às pessoas a possibilidade de usufruir dos direitos e liberdades clássicos, dessa vez em um ambiente virtual.

Em síntese, o impacto das tecnologias nas relações sociais e jurídicas atingiu o campo dos direitos fundamentais, fazendo-se tratar do debate sobre uma releitura dos direitos fundamentais em seu sentido clássico, necessitando, atualmente, de distintos modelos de proteção. É o que aponta Landa quando refere que:

El desarrollo de nuevas tecnologías permite a las industrias de las telecomunicaciones y la informática desarrollar cada vez más sofisticados sistemas, programas y aparatos de vigilancia electrónica, los cuales demandan nuevos estándares de protección de los derechos fundamentales, para evitar que se cometan excesos que afecten tanto a terceros como a los investigados, salvo en los casos en que sea estrictamente necesario. En el caso de que se cometan excesos, deben existir mecanismos de control sobre los privados, no únicamente estatales, sino también desde la ciudadanía y/o sus representantes en el Estado, por cuanto la interceptación y el almacenamiento de datos de las comunicaciones privadas en la era digital constituyen un grave peligro para los ciudadanos e incluso para las autoridades. (Landa, 2019, p. 155)

Observa-se que o panorama dos direitos fundamentais nas tecnologias é terreno arenoso diante das características próprias da Internet e das tecnologias e demonstra ainda mais a dificuldade de o Estado lidar com riscos próprios da Era da Informação, especialmente na sua atuação na esfera da segurança pública. Leal (2020) aponta, por exemplo, para a necessidade de encontros e sinergias entre as políticas de segurança e novos direitos como a proteção de dados pessoais, sobretudo em contextos de crise. Uma solução apontada por Landa (2018) é que a Internet impõe o cumprimento dos compromissos internacionais. Nas palavras do autor:

En la medida que los derechos fundamentales son universales, interdependientes e indivisibles, el internet los integra digitalmente y permite que trasciendan más allá de las fronteras de los Estados nacionales; no solo para el goce del mismo, sino también para su defensa y protección. Lo cual demanda que los Estados cumplan con sus compromisos internacionales de garantizar y promover los derechos humanos, en esta nueva era digital. (Landa, 2018)

Sobretudo, as liberdades são fortemente impactadas diante das novas tecnologias, especialmente como consequência das políticas criminais. Veja-se o notável risco a esse direito frente a mecanismos de reconhecimento facial em vias públicas, que permitem, por exemplo, a identificação e cruzamento com banco de dados de pessoas com mandados de prisão pendentes de cumprimento.

Verifica-se que a ampliação das tecnologias, marcadamente a Internet e a informática (aliadas às outras inovações a elas conectadas, quais sejam a microeletrônica, transmissão de dados, comércio eletrônico, entre outras), são fatores que impulsionaram transformações em variados aspectos no cenário constituído pelas redes e reforçado pelas novas tecnologias. Conforme leciona Bruno Cardoso (2018, p. 91):

O Estado seria, mais precisamente, um macroator constituído por uma pluralidade de atores menores e de conexões entre estes. A capacidade de construir redes (relativamente) estáveis entre (e com) esses atores, a partir da estabilização das relações que os conectam, garantindo que diversas cadeias de ação possam se desenvolver dentro de um certo nível de previsibilidade, é, assim, fundamental para a própria existência do Estado e para a efetividade de sua atuação.

Inevitável também é que inúmeros riscos foram erigidos a partir da Internet e da constituição de redes. A exacerbada vigilância estatal, sob o fundamento do combate ao terrorismo, por exemplo, a vigilância dos grandes conglomerados empresariais da tecnologia, a chamada economia de dados, podem ser alguns exemplos dos riscos que a tecnologia proporcionou. Esses riscos estão diretamente atrelados ao desenvolvimento e uso destas tecnologias pelos entes estatais, bastando verificar o crescente padrão desenvolvido após os atentados de 11 de setembro de 2001 e os reflexos na segurança nacional e segurança pública (Cardoso, 2018).

A vigilância nos dias atuais toca muitos aspectos da vida cotidiana: nossas casas, espaços de trabalho. Todos estes ambientes encontram-se tomados por inúmeros e sofisticados sistemas de coleta de dados e complexas tecnologias de vigilância com a presença do Estado Digital.

A despeito de que a maioria das pessoas não estejam conscientes disto, e da verdadeira dimensão do quanto estão sendo monitoradas/vigiadas, grande parte delas considera a vigilância como algo inexorável – quando não desejável – em suas vidas nos tempos atuais. E mesmo que se possa questionar a vida em uma Sociedade Viguada, resta indubitável que a propagação da vigilância tem dramaticamente alterado o modo pelo qual as comunidades funcionam e a convivência ordinária dos cidadãos diante da atuação do Estado.

Considerando o impacto nos direitos fundamentais em diversos aspectos, observa-se a necessidade de respostas teóricas pelo Direito aos novos fenômenos. Assim, surgem no Direito algumas correntes que pretendem estudar e analisar a crescente complexidade. O Constitucionalismo Digital se apresenta como “uma corrente teórica do Direito Constitucional contemporâneo que se organiza a partir de prescrições normativas e comuns de reconhecimento, afirmação e proteção de direitos fundamentais no ciberespaço” (Mendes; Fernandes, 2020, p. 5). Nesse sentido, Mendes e Fernandes (2020, p. 6) apontam que:

Dentro dessa perspectiva, pressupõe-se que a fruição de direitos fundamentais pode ser mediada pela força impositiva do Estado Nacional, ainda que em convivência com modalidades outras de conformação de direitos que têm origem na atuação de agentes privados ou no funcionamento de mecanismos transnacionais de governança da internet.

O Constitucionalismo Digital entende que a Internet e as suas tecnologias associadas possibilitam a realização das garantias individuais e que ela também é necessária para que muitos direitos sejam adequadamente fruídos (Mendes; Fernandes, 2020, p. 6). Nesse sentido, inúmeras propostas legislativas surgiram no Brasil, sendo o Marco Civil da Internet uma das principais no que diz respeito a normas que disciplinam a Internet, trazendo garantias de liberdade de expressão e pensamento, proteção à privacidade, desenvolvimento da personalidade (Brasil, 2014). Outra legislação a ser mencionada é a Lei Geral de Proteção de Dados Pessoais, que se pretende novel lei a tutelar os dados pessoais nos meios físicos e digitais (Brasil, 2018). Mendes e Fernandes (2020, p. 8) apontam que as iniciativas legislativas “consagram materialmente categorias de direitos, princípios e normas de governança para a internet, limitando drasticamente o poder de autoridades públicas e de atores privados nas suas relações com os usuários”.

Assim, a Internet – e as novas tecnologias que dela advém e com ela se relacionam – é uma garantia institucional da democracia e uma necessidade para que se goze plenamente dos direitos e liberdades previstos na Constituição e nos tratados sobre direitos humanos (Landa, 2019, p. 146). Entretanto, é preciso um ferramental de tutela a se iniciar no campo dos direitos fundamentais.

Grande parcela dos estudos, atualmente, deposita na proteção de dados pessoais o mecanismo atual de tutela da pessoa nos ambientes digitais. A complexidade nos direitos fundamentais diante das novas tecnologias e da amplitude que o direito à proteção de dados

personais assumiu na sociedade, faz com que alguns juristas a nominem como a preocupação jusfundamental de nosso tempo (Silveira; Froufe, 2018).

Nesse sentido, é possível verificar que:

A proteção dos dados pessoais alcançou uma dimensão sem precedentes no âmbito da sociedade tecnológica, notadamente a partir da introdução do uso da tecnologia da informática. [...] A facilidade de acesso aos dados pessoais, somada à velocidade do acesso, da transmissão e do cruzamento de tais dados, potencializa as possibilidades de afetação de direitos fundamentais das pessoas, mediante o conhecimento e o controle de informações sobre a sua vida pessoal, privada e social. (Sarlet; Marinoni; Mitidiero, 2017, p. 472).

Mecanismos de vigilância estatal e privada, uso no mercado para predição comportamental, bem como na economia da atenção (Freitas, Freitas, 2020), são pontos de destaque e preocupação presentes sobre o direito à proteção de dados e da privacidade. A questão ganha outros contornos quando se visualiza a privacidade no seio de riscos e perigos oriundos da Internet e desse desenvolvimento tecnológico. Como pontua Leal (2020, p. 366):

Nos dias atuais, os aspectos da tutela da privacidade e intimidade encontram-se muito integrados com a proteção de dados pessoais, pelo fato de que tais dados representam pressupostos irrenunciáveis ao desenvolvimento da pessoa humana e, ao mesmo tempo, estão conectados com demandas de mercado, pois alimentam infundáveis segmentos de atividades industriais e comerciais que pagam valores imensos por informações de seus consumidores, formatando-se, neste âmbito, zonas de potenciais conflitos entre interesses distintos.

Em tais cenários, as mutações ocorrem inclusive sobre os objetos de tutela jurídica envolvendo o direito à privacidade e intimidade, pois, da tradicional liberdade negativa (livre de ingerência externa), passa a ser integrado como bem tutelado o direito de autodeterminação informativa relacionada ao indivíduo e sujeito de direito. Ou seja, passa-se a reconhecer a todo o cidadão a faculdade de escolher o que deseja fazer com os seus dados pessoais – e o que não deseja também.

Cenários de maior risco à privacidade são a emergência e os Estados de Exceção, fundados, por exemplo, nas questões de segurança pública e de emergência sanitária, operadoras de restrições a esse direito fundamental, como aquelas vivenciadas no período da pandemia. Leal (2020, p. 361) traz o exemplo do Estado de Urgência promovido na França a partir de ataques em Paris, no ano de 2015, sob o fundamento da segurança pública e nacional, onde restou autorizada a promoção acesso a domicílios sem autorização judicial, devassando-se a privacidade do morador em nome de tais direitos.

Nesse sentido, Marion Albers (2018, p. 38) afirma:

A proteção de dados baseia-se em uma compreensão multidimensional de direitos fundamentais e exige descrições inteiramente novas dos interesses protegidos: em vez de bens juridicamente tutelados concebidos de modo individualista, a questão tem a ver com posições jurídicas individuais na socialidade ou, em outras palavras, as posições sociais do indivíduo a serem protegidas por direitos fundamentais. O conjunto de interesses e posições protegidos ainda precisa ser elaborado com maior grau de detalhamento e também terá de ser sempre adaptado dinamicamente a novos perigos.

Verifica-se que a questão é de importância global na atualidade em face dos mecanismos que utilizam dados pessoais para seu funcionamento. Normas e previsões legislativas específicas surgem como necessidade de se regulamentar a questão. Trata-se de mecanismos em sua maioria ou ainda não regulados, ou com legislações carentes por parte dos Estados. Atenta a estas preocupações, recentemente o Alto Comissariado das Nações Unidas aprovou relatório com diversas sugestões e recomendações aos Estados para o uso de tecnologias a partir da verificação das seguintes tendências pelos Estados: (a) o abuso generalizado de ferramentas intrusivas de hackeamento; (b) o papel fundamental de criptografia robusta para garantir o exercício do direito à privacidade e de outros direitos; e (c) o monitoramento generalizado dos espaços públicos (ONU, 2022).

Nesse sentido, é possível visualizar o surgimento do devido processo informacional, direito que regulamenta medidas legais e procedimentais para a forma com que dados pessoais serão tratados, uma vez que impactam diretamente nas liberdades individuais e coletivas (Bioni *et al*, 2020, p. 9), nomeadamente no que tange à segurança pública. A ausência de algumas diretrizes mínimas que devem estar presentes no tratamento de dados, especialmente pelo Estado, acarreta a fragilização das formas de operabilidade de tratamento, possibilitando concretos riscos à pessoa.

Assim, problemas referentes aos metadados, governo digital e inteligência artificial também devem ocupar a agenda do debate jurídico e político. Na atualidade, um desafio presente, como já referido, é a Inteligência Artificial (IA) e seu uso desmesurado nas atividades estatais – especialmente na segurança pública, causando o risco ou danos aos direitos fundamentais e esferas personalíssimas das pessoas. Basicamente, estruturas pautadas em inteligência artificial se utilizam de grandes bancos de dados (pessoais e não pessoais) e algoritmos para seu funcionamento.

Suas aplicações são as mais diversas. Como já referido, o presente artigo científico busca tracejar possibilidades de tutela de direitos fundamentais em um campo específico da IA: uso de tecnologias e inteligência artificial em atividades de segurança pública. Entretanto, antes de se adentrar na temática, é preciso fundar as bases mínimas para compreensão da atividade de segurança estatal, o que se faz no tópico seguinte.

3. Breves considerações sobre direito fundamental à segurança pública e reflexões contemporâneas

A segurança pública não é de há muito conferida como perspectiva de direito fundamental ou ao menos os trabalhos e pesquisas nesse sentido remontam a pouco menos de duas décadas no Brasil. Apesar de sua previsão constitucional no Brasil, essencialmente nos

artigos 5º, enquanto direito fundamental individual, e artigo 6º, enquanto direito fundamental social, o debate de sua definição vem sendo desenvolvido pelos teóricos para fins de delimitar competências e atribuições distintas dos órgãos estatais. A presente pesquisa parte da premissa de que a segurança pública é direito fundamental, tendo em vista que encontra amparo em nossa Constituição. Na lição de Leal e Gilioli (2018, p. 34):

O direito à segurança pública foi um dos direitos eleitos como fundamentais no texto constitucional e este direito não decorre por estar o mesmo instituído na Constituição como dever do Estado e uma responsabilidade de todos, mas essencialmente por se a segurança pública, através de políticas públicas executadas na área como forma de se materializar a garantia dos objetos jurídicos eleitos como fundamentais, tais como: a vida, a propriedade, a liberdade.

Na doutrina internacional, denota-se que a temática da segurança é de preocupação há muito tempo, principalmente os seus fundamentos políticos, sociais e institucionais (Torre, 2014). Não há preocupação da presente pesquisa em delimitar os pormenores do direito à segurança. Entretanto, necessário destacar seus fundamentos e possibilidades no campo teórico, diante do expressivo aumento do emprego de tecnologias nessa seara e sua relação com temáticas tecnológicas de preocupação jurídica.

A segurança pública é direito individual, na medida em que consagra a possibilidade subjetiva de tutela da pessoa, mas também se consagra como direito fundamental social, porquanto garante a possibilidade de tutela coletiva, difusa, entre outros. Assim, esse direito não assume, logo, uma feição coletiva ou individual, haja vista:

Com relação aos fundamentos constitucionais da segurança, é possível fazermos referência àquelas duas perspectivas já referidas, de um lado, a que lhe outorga a condição de interesse coletivo, e, de outro, a que lhe reconhece a condição de direito fundamental individual. Estas posições, todavia, não são irreconciliáveis, e devem estar associadas, e isto porque as dimensões individuais e coletivas/sociais das relações humanas, hoje e cada vez mais, contam com intersecções integracionistas, basta vermos o que ocorre nas chamadas redes sociais (Facebook, Instagram, WhatsApp, YouTube, Twitter, LinkedIn, Pinterest, Google+); tudo e todos estão interligados (Leal, 2020, p. 354).

Trata-se da tutela de uma existência digna protegida, com a fruição de outros direitos onde a coletividade e o indivíduo são titulares. Importante observar que, na condição de direito fundamental social, a segurança pública conclama a realização de ações positivas do Estado na sua promoção. Como bem pontua Novais (2010, p. 251):

Ser um direito fundamental significa, em Estado constitucional de Direito, ter uma importância, dignidade e força constitucionalmente reconhecidas que, no domínio das relações gerais entre o Estado e o indivíduo, elevam

o bem, a posição ou a situação por ele tutelada à qualidade de limite jurídico-constitucional à atuação dos poderes públicos.

Ou seja, sinergias entre o bem-estar coletivo e individual são basilares e essenciais para se estabelecer os parâmetros normativos e modos de tutela do direito à segurança pública, nomeadamente os limites legislativos, evitando-se arbitrariedades e ações ilegais. Trata-se de fundamento do Estado de Direito, nomeadamente pela *"la eliminación de la arbitrariedad en el ámbito de la actividad estatal que afecta a los ciudadanos."* (Zagrebelski, 1992, p. 21)

Em se tratando de segurança pública, constata-se tanto a função repressiva – revestida essencialmente da perspectiva de persecução penal, como de promoção, através da atividade estatal de tutela dos interesses e fruição das garantias individuais e coletivas. Feroni (2008) pontua que o direito fundamental à segurança é um valor superprimário imbricado com a vida, incolumidade física, bem-estar, qualidade da existência e dignidade humana. Na atualidade, constata-se que tal direito assume as feições na tutela dos interesses sociais, especialmente na proteção da vida humana e também dos limites privados.

Frosini aponta importante lição acerca da segurança como elemento jurídico de preocupação constitucional:

Se storicamente l'espressione "diritto alla sicurezza" poteva essere ritenuta una figura semantica a carattere retorico, oggi mi sembra che goda di uno status giuridico in parte autonomo - come diritto a un'esistenza protetta, indispensabile al godimento di altri diritti di cui un soggetto è titolare - e in parte indiretto, nel senso che è complementare agli altri diritti, ovvero come istanza radicata nella nozione di benessere e di qualità della vita, collettiva e individuale. Pertanto, la sicurezza può qualificarsi come bene inscindibilmente legato alla vita, alla incolumità fisica, al benessere dell'uomo e alla qualità della sua esistenza, nonché alla dignità della persona. Da ciò ne deriva che la sua titolarità oltre che in capo allo Stato, nella forma di interesse a garantire una situazione di pace sociale, è riferibile a ciascun individuo come diritto a un'esistenza protetta, indispensabile al godimento degli altri diritti di cui è titolare in condizioni di sicurezza.

No que toca ao desenvolvimento tecnológico, observa-se que o Brasil possui grave déficit na regulamentação dos instrumentos aplicáveis à segurança pública. Grande exemplo disso é o uso de dados pessoais no campo penal e a inexistência de previsões legislativas sobre o tratamento de dados pessoais na segurança pública e também na persecução penal.

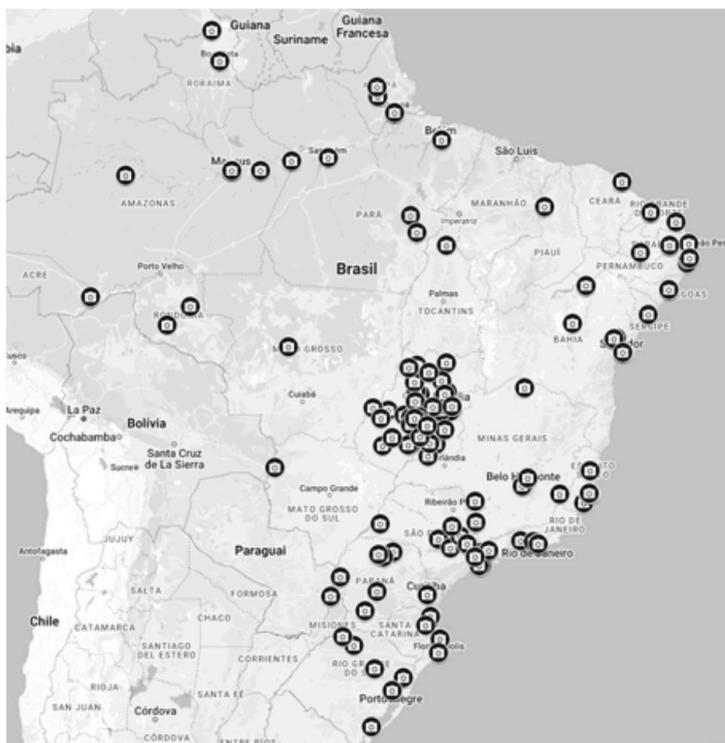
Destaca-se que as alíneas *a* e *d* do inciso III do artigo 4º da LGPD referem que a legislação em questão não é aplicável às atividades de segurança pública e de investigação e repressão a infrações penais, cuja regulamentação será de forma específica (Brasil, 2018). Surge, então, a iniciativa e necessidade de uma legislação própria que discipline a matéria, na busca de regulamentação das questões atinentes às investigações criminais, ações penais, prevenção de crimes. Leal acentua, da mesma forma, que a LGPD reservou espaço a uma legislação específica nessa matéria, referindo, porém, a existência de outros desafios relacionadas ao tema:

Ao mesmo tempo, em seu art. 4º, inc. III, a norma autorizou a flexibilização daqueles direitos para os fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais, sendo que o tratamento de dados pessoais previsto neste inc. III será regido por legislação específica, “que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei”. Por certo que aqui já temos outros desafios que é o de densificar materialmente – e no caso concreto – os níveis e possibilidades das *medidas proporcionais e estritamente necessárias* ao escopo da norma e diante de cenários os mais particulares existentes – como o da segurança da saúde pública na pandemia. (Leal, 2020, p. 368)

Em tal seara, há movimentação legislativa em relação à regulamentação. Todavia, trata-se tão somente de um anteprojeto de LGPD-Penal sem reflexo algum no cotidiano prático brasileiro. Inúmeros instrumentos são utilizados pelas atividades de segurança pública para fins de atingir os propósitos do direito fundamental. Cada vez mais o Estado, em sua atividade de segurança pública faz uso desses mecanismos para predição comportamental, mapeamento de áreas de maior insegurança e reconhecimento facial, por exemplo. Brandão e Arbix (2022) apresentam importante pesquisa sobre a aplicação da inteligência artificial no campo das políticas públicas de transporte, especialmente no uso de sistemas de reconhecimento facial. O estudo dos autores faz um levantamento de cidades brasileiras que utilizam IA para identificação de usuários de transporte público, com o objetivo de enfrentar e prevenir fraudes. A pesquisa constatou baixo nível de responsabilidade técnica e jurídica, considerando elevados os desafios de utilização desses mecanismos de modo responsável, inclusive diante das capacidades institucionais (Brandão; Arbix, 2022).

Nesse contexto, a figura abaixo, extraída de outro estudo, evidencia o amplo uso desses ferramentas em cidades do Brasil:

FIGURA 1. Mapeamento do uso de tecnologias de reconhecimento facial pelas forças de segurança



Fonte: Nunes, 2023

Trata-se, portanto, de questão que deve ser visualizada a partir de fatores complexos, uma vez que envolvem: proteção das pessoas contra agressões de terceiros; proteção da privacidade e dados pessoais; execução adequada de políticas públicas; uso de tecnologias para fins estatais.

Assim, percebe-se que a segurança pública se constitui como importante direito fundamental, de caráter individual e social, possibilitando a criação e efetivação de políticas públicas no contexto de atuação. Todavia, denota-se a necessidade de sinergias entre o uso das tecnologias, nomeadamente a inteligência artificial, frente aos mecanismos de tutela da segurança pública, conforme será adiante exposto.

4. Novas tecnologias, inteligência artificial e segurança pública: limites e desafios

Não há a pretensão da presente pesquisa em esmiuçar as aplicações e conceitos sobre IA no Brasil. O enfoque aqui conferido é tão somente analisar os desafios e sinergias entre

IA e segurança pública com o objetivo de tutelar a pessoa diante dos novos mecanismos, sobretudo no enfoque direitos fundamentais sociais e individuais. Em tais cenários, a equação sensível não é entre a liberdade e a segurança em tempos de ameaça, mas entre a segurança e a liberdade dos outros; ou seja, as liberdades de pequenos grupos suspeitos, como muçulmanos adultos do sexo masculino. Ao implementar medidas de vigilância em massa cria-se compensação diferente entre as liberdades civis e a segurança diante das ameaças. A questão que se segue, a partir disto, é: qual das liberdades as pessoas estão dispostas a sacrificar em nome da segurança pública? Trata-se de ponto fundamental de análise desta problemática, que será realizada, primeiramente, com breve enfoque conceitual.

Para fins conceituais, a inteligência artificial, como propõem Freitas e Freitas (2021, p. 30), é um “sistema algorítmico adaptável, relativamente autônomo, emulatório da decisão humana”. Basicamente, seu funcionamento decorre de um conglomerado de dados e uso de algoritmos para sua aplicação em situações específicas. Hoffmann-Riem (2022) afirma que, apesar dos enfoques teóricos atuais serem notadamente no uso de dados para vigilância estatal e por entes privados, a proteção jurídica não pode se limitar a eles, englobando, assim, todas as perspectivas que envolvam a tecnologia e o direito, especialmente a inteligência artificial.

Contudo, atualmente, o uso de Inteligência Artificial (IA) no âmbito dessas atividades de segurança se sobressai, especialmente através de videomonitoramento, captando imagens e informações de pessoas. Nesse sentido, se relacionados os dados pessoais e a inteligência artificial, pode-se obter informações importantes sobre a pessoa, pois os dados pessoais possuem papel fundamental no campo das análises obtidas com IA, pois, como acentua Doneda:

[...] os dados pessoais são tratados com o auxílio de métodos estatísticos e de técnicas de inteligência artificial, com o fim de se obter uma “metainformação”, que consistiria numa síntese dos hábitos, preferências pessoais e outros registros da vida desta pessoa. O resultado pode ser utilizado para traçar um quadro das tendências de futuras decisões, comportamentos e destino de uma pessoa ou grupo. (Doneda, 2019, p. 151)

Assim, denota-se que, para se conferir proteção à pessoa nesses cenários, importante a formação de políticas públicas, notadamente regulatórias. Schmidt (2018, p. 127) define política pública como “um conjunto de decisões e ações adotadas por órgãos públicos e organizações da sociedade, intencionalmente coerentes entre si, que, sob coordenação estatal, destinam-se a enfrentar um problema político”. Como um de seus instrumentos, pode-se citar a regulação através da via legislativa para a proteção dos direitos fundamentais (Reck, 2022).

No ponto aqui estudado, observa-se que se trata de um campo ainda não suficientemente protegido, especialmente a utilização de *Big Data* para o policiamento (Hoffmann-Riem, 2022, p. 151). Emerge, assim, a questão da limitação do poder estatal para se garantir a proteção à pessoa e, de outro lado, se garantir instrumentos efetivos e procedimentais nessa seara, uma vez que “a exigência de observar os requisitos do Estado de Direito ao realizar a vigilância do Poder Público continua sendo indispensável (Hoffmann-Riem, 2022, p. 151). O uso desses instrumentos não apenas define a prevenção de crimes,

mas o controle comportamental das pessoas e das ações policiais de repressão e prevenção (Hoffmann-Riem, 2022, p. 74).

Para além disso, em se tratando de uso de inteligência artificial por meio de algoritmos, há a crescente possibilidade de discriminação algorítmica, na medida em que boa parcela do tratamento de dados e informações nesse campo são feitas por mecanismos automatizados. Mendes e Mattiuzzo assim apontam que o debate “sobre discriminação algorítmica deve se centrar na seguinte ideia de que os valores que orientam a sociedade e o direito não podem ser deixados de lado quando falamos em automação e inteligência artificial” (2019, p. 61). Brandão e Arbix (2022), no estudo anteriormente referido, constatarem que existem diversos casos no mundo sobre a discriminação e preconceitos oriundos de algoritmos, nomeadamente em face de situações envolvendo reconhecimento facial para uso de segurança pública, a exemplo de bancos de dados com mandados de prisão pendentes de cumprimento.

Assim, exsurge a problemática da segurança pública e mecanismos legislativos para tutela da pessoa. Todavia, legislação federal alguma consta de previsões normativas específicas sobre o uso de videomonitoramento para fins de segurança pública. Trata-se, portanto, de balizar e verificar os direitos no choque de direitos entre a segurança pública e os dados pessoais:

De qualquer sorte, temos que o Direito Fundamental à Segurança da coletividade pode prevalecer, no Estado Democrático de Direito, sobre os direitos fundamentais da pessoa humana que, eventualmente, coloquem em risco ou provoquem danos a esta comunidade, mas tão somente no limite do necessário à restauração da segurança ameaçada/violada, prestando contas o Estado, por ação e omissão, dos seus atos (Leal, 2020, p. 167).

Veja-se que há visível conflituosidade entre os direitos, uma vez que não se oferecem soluções jurídicas específicas. Paralelamente, destaca-se que a LGPD oferece, por exemplo, o direito de explicabilidade de decisões tomadas de modo automatizado – reconhecimento facial com IA está nesse ponto. Entretanto, como já referido, a própria LGPD exclui sua aplicação em sede de segurança pública, inviabilizando o seu uso como fundamento para proteção da pessoa.

Atualmente, o país e o mundo buscam tratar da temática em sua perspectiva regulatória. Na União Europeia, trata-se do *IA Act*, mecanismo comunitário para tutela da IA na Europa. No Brasil, existem diversos projetos básicos com o mesmo objetivo, todavia sem aprovação em qualquer turno até o momento. Considerando a perspectiva adotada do presente trabalho, não se buscará analisar detidamente os casos brasileiros. Todavia, a fim de exemplificar o tratamento da questão no Brasil, em leitura do Projeto de Lei nº 2338/2023, ainda em tramitação preliminar no Senado Federal, o campo da inteligência artificial na atividade de segurança pública como de risco excessivo, possibilitando o seu uso ou por autorização judicial ou por autorização legislativa específica, prevendo medidas proporcionais e adequadas.

Denota-se que a necessidade regulatória é urgente, sob pena de violação a liberdades civis e direitos importantes do cidadão. Como bem advertem Freitas e Freitas (2020, p. 57) “ou a IA presta obséquio à liberdade intersubjetiva, ou não passa de instrumento de

desinteligência artificial e antinatural. Nada é mais urgente, no reino da regulação, do que direcionar sabiamente a IA". Necessária e urgente a formulação dos parâmetros normativos do uso de IA na segurança pública. Nesse sentido, em relação à regulação no uso de tecnologias e inteligência artificial para segurança pública, evidencia-se deficitária a proteção estatal.

5. Conclusões

O presente artigo teve por objetivo realizar uma análise das políticas de inteligência frente ao direito fundamental social da segurança pública. Do quanto foi exposto neste trabalho é possível extrair algumas conclusões e diretrizes sobre a temática. O texto discutiu a formulação de políticas públicas, especialmente no contexto da atividade de inteligência e segurança nacional, destacando a importância da participação democrática e da transparência.

Nesse contexto, é possível extrair algumas conclusões e diretrizes de aperfeiçoamento. A formulação de políticas públicas envolve decisões em todos os momentos e fases, o que destaca a complexidade e a importância do processo decisório, sendo crucial identificar e aperfeiçoar os modelos e agentes decisórios fundamentais para a política pública, garantindo a sua eficácia e legitimidade.

Nessa linha, a ampliação democrática evidencia uma necessidade de ampliar o aspecto participativo nas decisões, tanto nos objetivos e diretrizes quanto na estrutura organizacional, visando uma maior participação da sociedade. É sabido, nesse sentido, que a legitimidade das ações do Estado, especialmente na atividade de inteligência, ocorre pela comunicação e pela deliberação pública das ações e fundamentos da política pública.

Outro ponto conclusivo de extrema relevância é a regulamentação do tratamento e uso de dados pessoais para atividades de inteligência e de segurança pública é essencial para garantir a privacidade e a proteção dos dados. Trata-se de debate sobre a transparência e segurança nacional, pois apesar das questões sigilosas envolvendo a segurança nacional, é fundamental ampliar a transparência das políticas públicas, tornando-as reservadas e observadoras dos ditames de privacidade e proteção de dados.

Por fim, abrangendo todos os pontos vistos, a normatização é fator importante da política pública, podendo melhorar sua efetividade, especialmente considerando os direitos envolvidos durante todo o ciclo da política pública. Em suma, a formulação de políticas públicas, especialmente na área de inteligência e segurança, requer uma abordagem democrática, transparente e que respeite os direitos fundamentais.

Referências

ALBERS, Marion. A complexidade da proteção de dados. *Revista Direitos Fundamentais & Justiça*, a. 10, n. 35, p. 19-45, jul./dez. 2016.

ARROYO, César Landa. Derecho fundamental al Internet: contenido esencial. *Pensar*, Fortaleza, v. 23, n. 4, p. 1-22, out./dez. 2018. Disponível em: <https://periodicos.unifor.br/rpen/article/view/8447>. Acesso em: 01 ago. 2024.

BIONI, Bruno; EILBERG, Daniela Dora; CUNHA, Brenda; SALIBA, Pedro; VERGILI, Gabriela. *Proteção de dados no campo penal e de segurança pública: nota técnica sobre o Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal*. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2020.

BRANDÃO, R.; ARBIX, G Artificial Intelligence, Ethics and Public Policy— The Use of Facial Recognition Systems in Public Transport in the Largest Brazilian Cities. *Journal of Service Science and Management*, 15, p. 551-575, 2022, doi: 10.4236/jssm.2022.155032. Acesso em: 20 ago. 2024.

CARDOSO, Bruno. Estado, tecnologias de segurança e normatividade neoliberal. In: *Tecnopolíticas da Vigilância: perspectivas da margem*. São Paulo: Boitempo, 2018. p. 91-106.

CASTELLS, Manuel. *A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade*. Rio de Janeiro: Zahar, 2003.

_____. *A sociedade em rede*. 17. ed. rev. e ampl. São Paulo: Paz e Terra, 2016.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados*. 2. ed. São Paulo: Thomson Reuters, 2019.

FERONI, Cerrina. La sicurezza: un valore superprimario. In *Percorsi costituzionali: quadrimestrale di diritti e libertà*. Roma: Rubbettino, 2008.

FREITAS, Juarez; FREITAS, Thomas Bellini. *Direito e inteligência artificial: em defesa do humano*. 1. Reimpressão. Belo Horizonte: Fórum, 2020.

FROSINI, Tommaso Edoardo. Il diritto costituzionale alla sicurezza. In *Forum on line di Quaderni costituzionali*, acessado pelo sítio: http://www.forumcostituzionale.it/wordpress/wp-content/uploads/pre_2006/440.pdf, Acesso em 20 ago. 2024.

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

LANDA, César. (2016). Derecho fundamental al Internet. *Primeras Jornadas Nacionales de Derechos Fundamentales*. p. 1-26, 2016. Disponível em: <http://themis.pe/wp/wp-content/uploads/2016/07/Derecho-al-Internet-y-Libertad-de-Expresio%CC%81n.docx>. Acesso em: 01 ago. 2023.

_____. Contenido esencial del derecho fundamental a internet: teoría y praxis. *Libro homenaje del Área de Derecho Constitucional por los 100 años de la Facultad de Derecho de la Pontificia Universidad Católica del Perú Landa*. Lima: CICAJ, p. 145-173, 2019. Disponível em: <https://repositorio.pucp.edu.pe/index/bitstream/handle/123456789/169015/landa.pdf?sequence=1>. Acesso em: 15 ago. 2024.

LEAL, Rogério Gesta. Direito fundamental à proteção de dados em tempos de pandemia: necessárias equações entre segurança pública e privada. *Revista Brasileira de Direitos Fundamentais & Justiça*, Belo Horizonte, ano 14, n. 43, p. 357-374, jul./dez., 2020.

_____; GILIOLI, Volnete. *A segurança pública como direito fundamental social na sociedade de riscos: qual a função do direito penal?* Chapecó: Unoesc, 2018. LÉVY, Pierre. *Cibercultura*. 3. ed. São Paulo: Editora 34, 2010.

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. *Revista Brasileira de Direito*, Passo Fundo, v. 16, n. 1, p. 1-33, out. 2020. ISSN 2238-0604. Disponível em: <https://seer.imed.edu.br/index.php/revistadedireito/article/view/4103>. Acesso em: 01 ago. 2024. doi:<https://doi.org/10.18256/2238-0604.2020.v16i1.4103>.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. *Direito Público*, [S. l.], v. 16, n. 90, 2019. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766>. Acesso em: 01 ago. 2024.

NOVAIS, J. R. *Direitos sociais: teoria jurídica dos direitos sociais enquanto direitos fundamentais*. Coimbra: Coimbra Editora, 2010.

NUNES, Pablo. Vigilância da cor: a tecnologia de reconhecimento facial e sua utilização no Brasil. In: *Tecnologia, Segurança e Direitos: Os usos e riscos de sistemas de reconhecimento facial no Brasil*. Rio de Janeiro: Konrad Adenauer Stiftung, 2022. p. 35-60.

RECK, Janriê Rodrigues. *O direito das políticas públicas: regime jurídico, agendamento, formulação, implementação, avaliação, judicialização e critérios de justiça*. Belo Horizonte: Fórum, 2023.

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

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional*. 10 ed. rev. atual. e ampl. Porto Alegre: Livraria do advogado, 2010.

_____; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de Direito Constitucional*. 6. ed. São Paulo: Saraiva, 2017.

SCHMIDT, João Pedro. Para estudar políticas públicas: aspectos conceituais, metodológicos e abordagens teóricas. *Revista de Direito da UNISC*, Santa Cruz do Sul, v. 3, n. 56, p. 119-149, set/dez. 2018.

SILVEIRA, Alessandra; FROUFE, Pedro. Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão jusfundamental identitária dos nossos tempos. *UNIO – EU Law Journal*”, vol. 4, Nº. 2, julho/2018. Disponível em: <https://doi.org/10.21814/unio.4.2.2>. Acesso em: 04 ago. 2024.

TORRE, Alessandro (*a cura di*). *Costituzioni e sicurezza dello Stato*. Rimini: Maggioli Editore, 2014.

ZAGREBELSKI, Gustavo. *El derecho dúctil*. Torino: Giulio Einaudi, 1992.