Reconhecimento facial como política de segurança pública no estado da Bahia

Facial recognition as a public safety policy in the state of Bahia

ÉRICA NASCIMENTO PINHEIRO VARGAS

MÔNICA MATOS RIBEIRO

RESUMO

O objetivo deste artigo é descrever os principais benefícios e riscos da implementação da política pública de reconhecimento facial, via inteligência artificial, aplicada pela Secretaria de Segurança Pública no Estado da Bahia por meio dos projetos Vídeo Policiamento – Mais Inteligência na Segurança e Vídeo-Polícia Expansão. O estudo partiu do pressuposto da necessidade de mais acuidade na aplicação do reconhecimento facial, via inteligência artificial, para sua utilização como política pública de segurança, a fim de evitar possíveis violações de direitos fundamentais da liberdade, privacidade e proteção de dados pessoais. Buscou-se detalhar o impacto, nas políticas públicas, da aplicação das tecnologias de reconhecimento facial, via inteligência artificial, tendo como *locus* do estudo o estado da Bahia, pelo pioneirismo na sua implementação. A pesquisa é de natureza qualitativa, com abordagem de estudo de caso e técnicas de pesquisa bibliográfica e aplicação de questionário. Como resultado, observaram-se vantagens da política pública pesquisada, como (a) menor letalidade para os policiais e pessoas abordadas; (b) celeridade no reconhecimento de pessoas desaparecidas e foragidas da Justiça; e (c) inexistência, até a data de corte da pesquisa, de prisões motivadas por erros de reconhecimento facial na Bahia. Por outro lado, também foram demonstrados possíveis riscos de violação à liberdade, privacidade e proteção de dados pessoais, em razão da falta de transparência nos dados divulgados pelo governo do estado da Bahia e da ausência de regulamentação legal específica no Brasil sobre a referida política pública.

Palavras-chave: Segurança Pública. Reconhecimento Facial. Estado da Bahia.

ABSTRACT

The objective of this article was to describe the main benefits and risks of implementing the public policy of facial recognition, via artificial intelligence, applied by the Secretariat of Public Security in the State of Bahia through Vídeo Policiamento – Mais Inteligência na Segurança and Vídeo-Polícia Expansão projects. The study was based on the assumption of the need for more accuracy in the application of facial recognition, via artificial intelligence, for use as a public security policy, in order to avoid possible violations of fundamental rights of freedom, privacy and protection of personal data. We sought to detail the impact of information and communication technologies on public policies, based on the application of facial recognition technologies, via artificial intelligence, having the State of Bahia as locus of the study, due to pioneering spirit in its implementation. The research is of a qualitative nature, with a case study approach and techniques of bibliographical research and the application of a questionnaire. As a result, advantages of the researched public policy were observed, such as being (a) lower lethality for police officers and people approached; (b) speed in recognizing missing people and fugitives from justice; and (c) no existence, until the research cut-off date, of arrests motivated by facial recognition errors in Bahia. Possible risks of violation of freedom, privacy and protection of personal data were also demonstrated, due to the lack of transparency in the data disclosed by the govern of state of Bahia and the absence of specific legal regulation in Brazil.

Key words: Public Security. Facial Recognition. State of Bahia.

INTRODUÇÃO

O debate sobre segurança pública no Brasil, que já era recorrente, ganhou destaque quando da sua inserção em um dos capítulos da Constituição da República Federativa do Brasil de 1988, no qual está determinada a descentralização da segurança pública e a adoção da defesa dos direitos humanos e fundamentais. Além dessa determinação, o crescimento dos índices de violência corroborou com a elevação dos debates em âmbito público, privado e social, na busca por soluções efetivas.

Quando se observam dados referentes ao número de homicídios no Brasil, por exemplo, constata-se que entre 1990 e 2000 houve um aumento de aproximadamente 42% no número de homicídios no país. Entre 2000 e 2010, a elevação foi de 16,23%. E entre 2010 e 2017, o aumento foi de aproximadamente 24% (IPEA, 2023). Reduzir esses números e propor política de segurança pública que se mostre eficaz e respeite as determinações da Constituição Federal (CF) se tornaram um dos grandes desafios para o Estado brasileiro.

Em meios aos debates acerta da insuficiência de instrumentos de enfrentamento da violência e da criminalidade, foram adotadas no Brasil, a partir dos anos 2000, diversos programas e políticas públicas na área de segurança, tendo como mecanismo agregador a utilização das Tecnologias de Informação e Comunicação (TIC). A promoção de políticas

envolvendo as TICs se difundiu mediante estímulo à inovação tecnológica previsto no Plano Nacional de Segurança Pública (PNS) e à necessidade de o Estado brasileiro desenvolver novas ações preventivas e de combate à criminalidade (BRASIL, 2000). Conforme destaca Alcadipani (2020), o Brasil caminhou na direção da busca pelo desenvolvimento de estratégias e ações que envolvessem menos letalidade e mais ações de inteligência.

Nesse cenário, as TICs foram cada vez mais utilizadas nas políticas nacionais de segurança pública, como também passaram a estimular o aperfeiçoamento do sistema. Nesse sentido, para o aprimoramento das estratégias utilizadas, ocorreu o estímulo à utilização da Inteligência Artificial (IA), instituída pela PNS/2018, que trouxe a possibilidade de utilização do Reconhecimento Facial (RF) automatizado com o objetivo de fiscalização de fronteiras, rodovias, portos e aeroportos (BRASIL, 2018a).

Ainda no ano de 2018, o Estado da Bahia[1] foi pioneiro no Brasil na implantação do RF por IA como uma política de segurança pública e repressão ao crime, por meio do Projeto Vídeo Policiamento — Mais Inteligência na Segurança, cujo objetivo era o reconhecimento de pessoas em espaços públicos que tivessem mandados de prisão expedidos pela Justiça ou ainda para identificação de pessoas desaparecidas e de placas de veículos (BAHIA, 2019a).

Assim, a Secretaria de Segurança Pública do Estado da Bahia (SSP-BA) instalou câmeras de videomonitoramento com RF em lugares de grande circulação de público com o objetivo de prevenir e reprimir a criminalidade (BAHIA, 2019b). Apresentada pelo estado como *case* de sucesso, essa política pública alcançou, no primeiro semestre de 2023 — cinco anos depois de implementada —, o número de 900 prisões de pessoas foragidas da justiça, sendo investidos ao longo desse período, aproximadamente, R$ 650 milhões. O RF automatizado continua em expansão na Bahia, com a proposta de instalação de câmeras de segurança em mais 80 cidades do interior do Estado (BAHIA, 2023).

Apesar da apresentação de resultados eficientes quanto à operacionalização da referida política, deve-se atentar para algumas questões sensíveis. A compatibilização desta com os direitos da privacidade e proteção de dados pessoais, em atenção à Lei nº 13.709/2018 (BRASIL, 2018b), chamada Lei Geral de Proteção de Dados Pessoais (LGPD), é uma delas. Uma vez que que a ferramenta só pode funcionar mediante sua

[1] O Estado da Bahia já aplicava desde 2008 o videomonitoramento por Circuito Fechado de Televisão (CFTV) como política pública de segurança.

aplicação indiscriminada — ou seja, a quaisquer pessoas que passassem pelo sistema de videomonitoramento —, há que se considerar a possibilidade de violação da liberdade das pessoas.

Entre outros pontos que mereceram reflexões está o fato de que, por se tratar de uma tecnologia, a IA do RF poderia sofrer limitações técnicas de acurácia e confiabilidade que impactariam a assertividade do reconhecimento das pessoas (OLIVEIRA, 2021; RUBACK; AVILA; CANTERO, 2021; SILVA JÚNIOR, 2020). A essas questões se somam a presença de possíveis vieses raciais e sexistas dos algoritmos que poderiam implicar erros na adoção do RF como política pública, principalmente para pessoas negras, mulheres e transexuais (BUOLAMWINI; GEBRU, 2018; NOBLE, 2018; NORRIS; ARMSTRONG, 1999; SILVA, S., 2020).

Dessa maneira, diante da possibilidade de possíveis falhas na aplicação dessa política pública, que pode levar inocentes a serem presos indevidamente, é importante trazer à baila a possibilidade de a utilização da referida tecnologia provocar consequências de possíveis violações aos direitos da liberdade, privacidade e proteção de dados pessoais (NEGRI; OLIVEIRA; COSTA, 2020; RODOTÀ, 2008; SOLOVE, 2011b; WERTHEIN, 2000).

Assim, em razão da sensibilidade e relevância do tema, pelo alcance dos efeitos sociais da multicitada política pública, este artigo tem como objetivo principal descrever os benefícios e riscos da utilização da tecnologia do RF como política de segurança pública pelo estado da Bahia, frente às garantias e desenvolvimento dos direitos fundamentais da liberdade, privacidade e proteção de dados pessoais. Para alcançar o objetivo, foram apresentados e discutidos os projetos Vídeo Policiamento – Mais Inteligência na Segurança e Vídeo-Polícia Expansão, implementados pelo estado em 2018 e 2019, respectivamente.

No que tange à metodologia, caracteriza-se como uma pesquisa de natureza qualitativa, com abordagem de estudo de caso, sendo estudados os projetos Vídeo Policiamento – Mais Inteligência na Segurança e Vídeo-Polícia Expansão, implementados pela SSP-BA, nos anos de 2018 e 2019, respectivamente. Além da técnica de pesquisa bibliográfica, foi utilizado também um questionário, com dez questões abertas, respondidas pela Ouvidoria Geral do Estado da Bahia[2]. A Ouvidoria foi o órgão indicado, em consulta

[2] As questões foram enviadas via preenchimento de requerimento no sítio eletrônico: http://www.ouvidoria.ba.gov.br/, no dia 10 de novembro de 2021, por meio da Assessoria Técnica – SSP/GAB/SGTO/ASTEC, sob a manifestação nº 2502646, Doc. SEI 00038081895, protocolada sob o nº 409, em que se questiona a utilização do RF como política de segurança pública no Estado da Bahia.

realizada através da Lei de Acesso à Informação, como responsável para responder questões pertinentes ao tema.[3]

O artigo está organizado em quatro seções, incluindo esta introdução. A segunda seção dedica-se às tratativas sobre a inserção das TICs nas políticas públicas de segurança no Brasil. A terceira seção trata sobre a utilização da política de RF com base nos direitos fundamentais da liberdade, privacidade e proteção de dados pessoais. A quarta seção é dedicada à descrição das políticas públicas de RF, via IA, aplicadas pelo estado da Bahia por meio do programa Vídeo Policiamento — Mais Inteligência na Segurança e Vídeo-Polícia Extensão. Nas considerações finais são apontadas as limitações e perspectivas de estudos futuros.

1. POLÍTICA DE SEGURANÇA PÚBLICA NO BRASIL E O USO DA TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO

A criação da Intendência Geral de Polícia e Corte do Estado do Brasil, em 1808, na cidade do Rio de Janeiro, inaugurou a ação da segurança pública sob a égide do Estado. Desempenhando a função de polícia jurídica, exercia também as funções de delegação, fiscalização e aplicação de punições, segundo Marcineiro e Giovanni (2005). O Observatório de Segurança Pública (2020) destaca que, quando o Brasil promulgou sua primeira Constituição, em 1824, seu Código Criminal (1830) e um código voltado para o Processo Criminal (1832), a lei penal passou a ser compreendida como infração penal, e as penas de degredo e a privação de liberdade substituíram o sofrimento físico.

As Constituições subsequentes, promulgadas em 1934, 1937 e 1946, somadas ao Código Penal, de 1940, e ao código de Processo Penal, de 1942, imprimiram mudanças na segurança pública nacional, ao estabelecerem normas referentes aos crimes que passaram a ser centralizados pela administração pública. Entretanto, conforme destaca o Observatório de Segurança (2020), a Ditatura Militar relegou, mediante torturas e degradações, os direitos constitucionais dos investigados e capturados pela polícia.

Com a promulgação da denominada Constituição Cidadã, em 1988, a segurança pública passou a ser consagrada como direito fundamental, como se lê no Art. 144, "A

[3] Não foram utilizados nesta pesquisa dados de ações judiciais, que poderiam subsidiar os debates, porque consultas de dados consolidados no TJ-BA e instâncias superiores, entre 2018 e 2022, indicaram apenas duas ações judiciais em que houve o questionamento da legalidade do RF por IA, com resultado negativo para os autores, e uma ação judicial do RF por videomonitoramento por CFTV.

segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem púbica e da incolumidade das pessoas e do patrimônio" (BRASIL, 1988). A CF também descentralizou a segurança pública, através da atribuição de responsabilidades à Polícia Federal; Polícia Rodoviária Federal; Polícia Ferroviária Federal; polícias civis; polícias militares e corpos de bombeiros militares; e polícias penais federal, estaduais e distrital.

Apesar da configuração social-político-institucional definida pela nova Constituição, não ocorreu a desejada integração entre as práticas das polícias e do Judiciário, no que tange às ações punitivas, e os direitos humanos e sociais definidos pela Carta Magna (VARGAS; RIBEIRO, 2023). Não foi observada uma política de segurança pública democrática, preconizada por um Estado democrático de Direito. O que se observou foi a elevação exponencial das iniciativas privadas na área da segurança, ou seja, uma crescente privatização da mesma (BARBOSA, 2018), além do crescimento da criminalidade e da violência no Brasil (IPEA, 2023).

Conforme destacado pelo Observatório de Segurança (2020), como solução para o crescimento da violência o estado investiu em armas e equipamentos, elevando o manancial armamentista e ampliando os instrumentos de controle da sociedade. Por outro lado, a sociedade passou a se proteger com a construção de muros, condomínios fechados, gradeamento das casas e estabelecimentos comerciais, instalação de dispositivos eletrônicos, contratação de segurança privada, dentre outras ações. Instalou-se na sociedade a cultura do medo e a sensação de insegurança, particularmente, nos grandes centros urbanos, além, conforme destacam Carvalho e Silva (2011), de um processo de "criminalização da pobreza e da miséria", fruto da precarização das relações sociais de produção advinda do Estado neoliberal.

Agrega-se a esse complexo contexto o uso cada vez mais intensivo de tecnologias por parte dos criminosos. Como destaca Alcadipani (2020, p. 1): "Como criminosos sempre buscam minimizar o risco de serem presos ao praticar o delito e maximizar o seu retorno, os atuais desenvolvimentos tecnológicos serão incorporados cada vez mais na prática cotidiana dos que praticam crimes". Ressalta Alcadipani (2020, p. 1) que as forças de segurança pública precisam se preparar para esse cenário. Ao Estado, cabe investir e aprimorar conhecimentos, tecnologias, treinamentos, para que possa ter "[...] mais policiais que dominem a lógica das tecnologias digitais" (ALCADIPANI, 2020, p. 1).

Diante desse complexo cenário, o uso das TICs passou a ser uma exigência nas políticas públicas, particularmente as de segurança. O Estado passou a desenvolver planos

com o objetivo de estabelecer diretrizes, princípios e instrumentos para a implementação de políticas com a previsão de "melhorar a governança do setor público, aumentando a eficiência e eficácia das ações de governo" (BRASIL, 2018a, p. 20), almejando qualificar a segurança pública para o combate à criminalidade no país e para a promoção da segurança para a população.

Como analisam Carvalho e Silva (2011, p. 62), o sistema de segurança pública desenvolvido a partir da CF de 1988 "[...] tem servido apenas de paliativo a situações emergenciais, sendo deslocadas da realidade social, desprovidas de perenidade, consistência e articulação horizontal e setorial". Carvalho e Silva (2011, p. 62) continuam:

> [...] somente uma década após a promulgação da "Constituição Cidadã" [...] a política de segurança pública passa a ser pensada sob o contexto de uma sociedade democraticamente organizada, pautada no respeito aos direitos humanos, em que o enfrentamento da criminalidade não significa a instituição da arbitrariedade, mas a adoção de procedimentos tático-operacionais e político-sociais que considerem a questão em sua complexidade.

Assim, no ano de 2000 foi criado o PNS/2000, sendo, inclusive, considerado como a primeira política de segurança com estímulo à inovação tecnológica, uma ação estratégica importante para a eficácia e eficiência do sistema. Lopes (2009) destaca que o Plano propôs o aperfeiçoamento do sistema de segurança pública ao integrar as políticas de segurança, sociais e ações comunitárias, organizando um novo modelo de segurança pública, como também buscando reprimir e prevenir a violência e a criminalidade no Brasil.

Os tímidos avanços do PNS/2000, alinhados aos problemas de financiamento, de fragilidade na definição das metas e da avaliação de eficiência, eficácia e efetividade, levaram à criação de outros programas e políticas na área de segurança, ensejados, também, pela percepção de contínua e crescente violência e criminalidade no país. Assim, entre os anos de 2003 e 2017, foram criados programas e políticas voltados para restaurar a ordem pública, articular ações policiais e da justiça criminal, e garantir a integridade física e patrimonial das pessoas: em 2004, a Força Nacional de Segurança Pública; em 2007, o Programa Nacional de Segurança com Cidadania (Pronasci), que tinha como objetivo promover o financiamento de ações de prevenção a violência; em 2012, o Plano Brasil Mais Seguro, que objetivava reduzir a criminalidade violenta no país; em 2015, o Plano Nacional para Redução de Homicídios (BRASIL, 2018a, p. 34).

No que se refere ao fomento para a inovação, destaca-se a publicação da Lei nº 12.258/2010 (BRASIL, 2010), que, ao alterar o Código Penal e a Lei de Execução Penal, possibilitou a utilização de equipamento de vigilância indireta (monitoração eletrônica[4]), por condenados pela justiça, para os casos de saída temporária do regime semiaberto e para o cumprimento de pena em regime domiciliar. No ano de 2011, o Código de Processo Penal foi modificado, com a publicação da a Lei nº 12.403, instituindo o monitoramento eletrônico como medida cautelar (VIDAL, 2014).

A Lei nº 12.681, de 4 de julho de 2012 (BRASIL, 2012), instituiu o Sistema Nacional de Informações de Segurança Pública, Prisionais e sobre Drogas (Sinesp), que avançou nos aspectos tecnológicos ao integrar em uma plataforma de informações as bases de dados dos governos federal e dos estados, com o objetivo de criar uma estrutura de gestão de informação em nível nacional, para armazenar e tratar dados e informações que auxiliassem na formulação, implementação, execução, acompanhamento e avaliação das políticas de segurança pública, sistema prisional e enfrentamento do tráfico de drogas ilícitas (SANTOS; LIMA; SOUZA, 2020). Santos, Lima e Souza (2020) tecem uma crítica ao Sinesp, destacando que o imprescindível envolvimento "ativo" de todas as unidades federativas não foi acompanhado pela observância das diferentes realidades concernentes aos aspectos culturais, técnicos e orçamentários das mesmas.

Cabe destacar que, em 2012, o Ministério da Justiça, objetivando otimizar os recursos públicos e promover ações de fomento para a segurança pública, publicou o Edital Público 2012, no qual compunha um guia para apresentação de propostas para o desenvolvimento de convênios entre o governo federal e os estados e municípios. A proposta era direcionar recursos do Fundo Nacional de Segurança Pública para ações de prevenção da criminalidade. Como indica Freitas Filho (2018), o guia tinha como destaque o incentivo à implantação e/ou expansão do videomonitoramento no país, transformando-se em um marco para o seu desenvolvimento, ao destinar recursos específicos para essa tecnologia.

No ano de 2018, buscando consolidar como instrumento de Estado a Política Nacional de Segurança Pública, foi publicado o Plano Nacional de Segurança Pública de Desenvolvimento Social 2018-2023 – PNS/2018 (BRASIL, 2018a). Referido Plano criou o Sistema Único de Segurança Pública (Susp) para o desenvolvimento de governança, "[...] através da padronização de dados, integração tecnológica, de inteligência e operacional"

[4] Esse não é um debate pacífico. Há quem defenda essa prática e quem o considere um retorno ao Estado totalitário (KARAM, 2007).

(BRASIL, 2018a, p. 3), sendo considerado um novo estímulo para o uso de tecnologias na segurança pública, e, no dizer do então ministro da Segurança Pública Raul Jungmann, algo capaz de "[...] preencher um vácuo de quase dois séculos" e de abrir "a real possibilidade" de finalmente o país contar "com uma Política Nacional de Segurança Pública" (BRASIL, 2018a, p. 4).

No PNS/2018 o RF biométrico passou a ser estimulado, sendo indicada no objetivo/estratégia nº 8 a utilização de referida tecnologia como política de segurança pública para fiscalização de fronteiras, divisas interestaduais, portos, aeroportos, rodoviárias e ferrovias (BRASIL, 2018a, p. 57). O estado da Bahia foi pioneiro na implementação do RF como política de segurança pública, já no ano de 2018.

Fragilidades identificadas no PNS/2018, para tornar a sua implementação, monitoramento e avaliação factíveis, levaram o estado a publicar, em setembro de 2021, o Plano Nacional de Segurança Pública e Defesa Social 2021-2030 — PNS/2021 (BRASIL, 2021). Dentre as ações estratégicas do PNS/2021, destacam-se as voltadas para incentivar medidas que promovam a modernização e expansão tecnológica de equipamentos, e ações investigativas e de perícia, na busca pela integração, padronização e interoperabilidade dos dados entre União, Estados, Distrito Federal e Municípios. Uma dessas ações refere-se ao fomento à utilização de ferramentas de aprendizado de máquina (*machine learning*) para categorização e análise de dados. A estratégia nº 8 do PNS/2021 também prevê o fortalecimento das atividades de inteligência nas instituições de segurança pública e defesa social, com o objetivo de analisar, gerir e compartilhar dados e informações, através da atuação do Susp.

Outra iniciativa voltada para o uso de tecnologias na segurança pública, que ganhou destaque em 2021, refere-se ao uso de câmeras corporais nos uniformes dos policiais. Denominada de câmeras *body-worn*, a tecnologia que acopla câmeras em uniformes, capacete ou óculos dos policiais tem a capacidade de captar e gravar imagens e áudios das atividades desenvolvidas por policiais na sua rotina de trabalho. O estado de São Paulo foi pioneiro na adoção da prática, sendo replicado por outros estados, a exemplo do Rio de Janeiro e Santa Catarina.

Para Alcadipani, Bueno e Lima (2021), os resultados do uso das câmaras corporais "[...] são positivos para a profissionalização da polícia, com redução da letalidade e preservação de provas nas ações policiais". Para Duarte (2022), sob a ótica da sociedade civil, as imagens podem ajudar na garantia da disciplina e evitar abuso de autoridade, além

de proporcionarem segurança aos agentes. Outros defensores argumentam que seu uso eleva a transparência, a legitimidade policial e a coleta de provas, além da resolução célere de queixas. Por outro lado, autores como Albardeiro (2020) questionam a violação da privacidade dos cidadãos e dos policiais, assim como, a intimidação das ações pelos policiais e a própria vítima[5].

Pode-se assim observar, que o uso da tecnologia vem avançando, desde os anos 2000, nos Planos Nacionais de Segurança Pública adotados pelo Brasil, particularmente o uso do RF. Nesse sentido, faz-se necessário analisar se tais políticas não violam direitos fundamentais da liberdade, privacidade e proteção de dados pessoais.

2. RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA SOB O OLHAR DOS DIREITOS FUNDAMENTAIS

A CF enumera, em seu artigo 5º, a consagração dos direitos da inviolabilidade à vida, à liberdade, à igualdade, à segurança e à propriedade aos brasileiros e estrangeiros residentes no país. Destaca-se a previsão do artigo 5º, quando dispõe que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988).

Em 10 de fevereiro de 2022, a proteção dos dados foi incluída na CF, como direito fundamental autônomo, através da Emenda Constitucional nº 115 (BRASIL, 2022), que tornou a proteção de dados pessoais, inclusive nos meios digitais, um direito fundamental, com a inclusão do inciso XII-A, no artigo 5º. Os direitos fundamentais se revestem na forma de princípios e garantias da pessoa; nesse sentido, a elevação de um direito para o nível de fundamental é fortalecê-lo quanto a sua aplicação e reivindicação (VARGAS; RIBEIRO, 2020).

Ao considerar as tecnologias de IA de RF na segurança pública, a justificativa dos gestores públicos é o cumprimento do direito fundamental de segurança previsto na CF. Para João, Lunardo e Cristiano (2016, p. 27),

> [...] os governantes, no sentido de responder a essa preocupação relacionada com a segurança enquanto política pública, apresentaram ações de caráter restritivo e aporético aos demais direitos fundamentais,

[5] Nota da edição: para um levantamento bibliográfico dos ganhos e perdas envolvidos no uso de câmeras corporais, ver "Examinando câmeras corporais: uma revisão da literatura e balanço dos estudos empíricos", de David Pimentel Barbosa de Siena, neste mesmo volume.

> como: sistemas de vigilância, leis penais mais severas, controle de imigração etc.

Ainda segundo João, Lunardo e Cristiano (2016, p. 17), as ações acima "[...] polarizam as duas reivindicações da sociedade, que são a garantia dos direitos individuais e a emergência do direito à segurança" e se refletem na adoção de políticas públicas de segurança, como o RF por IA, que urge ser vista sob a ótica da liberdade, privacidade e proteção de dados pessoais.

2.1 Liberdade

A liberdade é considerada um direito fundamental e está previsto na CF de 1988 em seu artigo 5º, no mesmo patamar de proteção da segurança e da privacidade. Para Silva, J. (2008, p. 235), a liberdade pode ser classificada em cinco grupos:

> 1) Liberdade da pessoa física (liberdade de locomoção, de circulação); 2) Liberdade de pensamento, com todas as suas liberdades (opinião, religião, informação, artística, comunicação do conhecimento); 3) Liberdade de expressão coletiva em suas várias formas (de reunião, de associação); 4) Liberdade de ação profissional (livre escolha e de exercício de trabalho, ofício e profissão); 5) Liberdade de conteúdo econômico e social.

As tecnologias de RF automatizadas, baseadas em algoritmos cada vez mais inteligentes, se destacam enquanto ferramentas empregadas para fins de vigilância cuja onipresença torna-se cada vez mais evidente e que podem afetar a liberdade de locomoção e expressão, se não estiverem regulamentadas e controladas. Contudo, há grande naturalização na sociedade quanto a seu uso, sem grandes mobilizações populares quanto aos possíveis efeitos nocivos e abusivos deste tipo de tecnologia, porque muitas pessoas não se sentem ameaçadas ou vigiadas — ilusão da liberdade (NEGRI; OLIVEIRA; COSTA, 2020, p. 2).

As pessoas que resistem ao sistema, por outro lado, podem sofrer o chamado *chilling effect* — efeito em que o exercício da liberdade pode implicar uma sanção, fato que pode desencorajar e inibir o exercício legítimo de direitos à liberdade de expressão, associação, reunião e manifestação política (SOLOVE, 2011a; OLIVEIRA, 2021). Para Silva, P. (2020, n.p.), o RF é uma das tecnologias

> [...] emergentes de IA de maior potencial lesivo aos direitos humanos. Ela pode ter consequências perversas dependendo da finalidade para qual é

> implementada, principalmente quando desproporcionalmente utilizada pelos governos para vigilância e policiamento.

Quanto à utilização da IA frente ao princípio da liberdade e suas possíveis classificações, cumpre observar também a previsão do Marco Civil da Internet (MCI), Lei nº 12.965/2014 (BRASIL, 2014), que estabelece princípios, garantias, direitos e deveres para a utilização da internet no Brasil. Uma vez que a IA, em regra, necessita de internet, essa legislação seria plenamente aplicável (DRUMMOND; CARNEIRO, 2022).

O MCI apresenta como fundamento o direito à liberdade de expressão, a livre iniciativa, a livre concorrência e a defesa do consumidor. Entre outros princípios dispostos no MCI, está o respeito aos direitos humanos. Assim, o "Marco Civil fortalece uma visão antropocêntrica da IA (*human-centered AI*), posicionando a condição humana no centro das discussões sobre a revolução tecnológica" (DRUMMOND; CARNEIRO, 2022).

Apesar da liberdade de estabelecimento de novos negócios na internet, prevista no artigo 3º, do MCI (BRASIL, 2014), a permissão do desenvolvimento de aplicações na rede e da utilização desta como fonte de dados para outras aplicações tem que ser compatibilizada com os limites legais impostos, a exemplo da liberdade de expressão, privacidade e proteção de dados pessoais (DRUMMOND; CARNEIRO, 2022).

Assim, a IA — notadamente o *negócio* RF — é prevista como exercício da liberdade previsto no MCI. Contudo sua utilização, ainda mais para efeito de uma política pública, tem que respeitar a liberdade de locomoção, expressão, sob pena de o monitoramento constante e ostensivo extinguir o "agir livre", e consequentemente, a liberdade individual (OLIVEIRA, 2021).

2.2 Privacidade

O direito à privacidade está previsto no artigo 5º da CF: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". Também o artigo 21 do Código Civil o considera um direito fundamental e direito da personalidade, uma figura jurídica que supera a dicotomia entre direito público e privado (CANCELIER, 2017, p. 222; DONEDA, 2006). A CF positiva o direito da "proibição de interferência estatal na vida privada, exceto excepcionalmente, desde que de acordo com a lei, por razões importantes e legítimas de interesse público" (ARANHA; FERREIRA, 2020).

O MCI previu o direito à privacidade no ambiente digital como princípio, ao estabelecer a garantia do direito à liberdade e privacidade nas comunicações como condição

para o uso da internet no Brasil. Com o desenvolvimento da tecnologia, a partir da segunda metade do século XX e, principalmente, em vista do crescimento do volume de informações e da variedade das tecnologias que exploram a coleta e sensoriamento, o conceito de privacidade passa a denotar mudanças, no sentido de ser ampliado, alcançando novos sujeitos em razão da modificação social da relação das pessoas com os espaços públicos e privados (CANCELIER, 2017; DONEDA, 2006).

A preocupação com a privacidade avançou, na medida em que cada vez mais as tecnologias da informação se encontram nas mãos das grandes empresas e dos governos, e podem ser utilizadas para fins de vigilância e controle das massas. Ressalta-se, entretanto, que "a proteção da privacidade não implica necessariamente a destituição de medidas de segurança, mas estas devem ser supervisionadas" (OLIVEIRA, 2021, p. 99).

A falta de regulação legal de algumas tecnologias, a vigilância ostensiva e erros decisórios das máquinas que impactam na vida das pessoas, bem como a desigualdade quanto ao controle das informações e acesso a elas — que podem estar concentrados no Estado, em países ricos e/ou em empresas de tecnologias — também são desafios para a chamada sociedade da informação no que tange à democratização do acesso às tecnologias da informação e comunicação e, consequentemente, do poder de controle (WERTHEIN, 2000).

A massiva coleta de dados pessoais gera danos e apresenta outro problema, qual seja, a exclusão que acontece quando as pessoas ficam impedidas de ter conhecimento sobre os seus dados para saber como eles estão sendo utilizados, até mesmo para corrigi-los, se for o caso — por exemplo, na aplicação de análise de cadastro para saber se tem direito a um benefício de determinada política pública e, principalmente, nas questões relacionadas a medidas de segurança nacional e segurança pública (SOLOVE, 2011b).

A falta de conhecimento sobre a utilização de seus dados leva a uma desestruturação estrutural na forma como as pessoas são tratadas pelas instituições, criando um desequilíbrio na relação de poder entre as pessoas e o governo. "Até que ponto os funcionários do governo deveriam ter um poder tão significativo sobre os cidadãos?", questiona Solove (2011a, p. 7), concluindo que o problema da utilização dos dados pessoais não é o que as pessoas têm a esconder, mas sobre poder, estrutura e governo.

Dessa maneira, é cada vez mais importante o estabelecimento dos direitos fundamentais da privacidade e da proteção dos dados pessoais como um direito autônomo, que proteja os titulares da utilização massiva de seus dados pessoais de forma a manipulá-

los quanto ao seu consumo, vida privada, liberdade e interesses das empresas privadas e governos.

2.3 Proteção de dados pessoais

Na sociedade da informação e vigilância, em que os dados pessoais têm um caráter valioso na personalização de produtos e serviços e as maiores empresas do mundo atualmente trabalham com mineração de dados, proteger os dados pessoais deve ser um direito fundamental por se tratar da "dimensão relacional da pessoa humana" (BIONI, 2018). A proteção de dados se fundamenta na preservação da individualidade, liberdade e democracia (OLIVEIRA, 2021, p. 115).

Conforme o artigo 5º da LGPD, os dados pessoais são "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018b). Assim, são considerados dados pessoais o nome, Cadastro de Pessoa Física (CPF), endereço, a raça, gênero, orientação sexual, a biometria, dentre outros, sendo esta última, que é o objeto do videomonitoramento automatizado na segurança pública, considerada um dado sensível, em que se deve prover ainda mais proteção em razão de sua natureza.

Assim, segundo Aranha e Ferreira (2020, p. 2), "enquanto o direito à privacidade consiste em uma proibição geral de interferência estatal, o direito à proteção de dados pessoais é um direito novo e ativo, que impõe o funcionamento de um sistema de segurança para proteger o indivíduo sempre que seus dados pessoais são coletados e utilizados". Trata-se, portanto, de uma questão de extrema relevância por envolver dados de IA pelo RF para fins de segurança pública.

É importante ressalvar que, em uma leitura inicial, a LGPD não seria aplicável ao tratamento de dados exclusivos para segurança pública, defesa nacional, segurança do Estado e repressão de infrações penais, o que não poderia ser invocada para o presente trabalho quando trata da aplicação da IA de RF na segurança pública do estado da Bahia. Destaca-se que, ao fazer uma análise interpretativa da LGPD, se defende a aplicação da lei em alguns requisitos, principalmente no que tange às questões principiológicas (BLUM; LOPEZ, 2020, p. 173), ou seja, a princípios que regem esta lei e que devem ser obedecidos pelo Poder Público, a exemplo do que dispõe o parágrafo primeiro do artigo 4º da LGPD: finalidade, adequação, necessidade, transparência e não-discriminação, assim como os direitos de acesso aos dados, correção, anonimização, e eliminação de informações inadequadas – artigos 6º, 17 e 18, da referida lei.

Assim, é imprescindível que a administração pública também haja com precaução (BIONI, 2018) quando da contratação e utilização de tecnologias, a exemplo do RF, que podem ser

mais invasivas aos direitos individuais. Uma vez que pode ocasionar o controle de massas para fins políticos, econômicos e ideológicos e, por consequência, impactar os direitos fundamentais da liberdade, privacidade e proteção de dados pessoais, essa política pública precisa ser regulamentada.

3. RECONHECIMENTO FACIAL COMO POLÍTICA DE SEGURANÇA PÚBLICA NO ESTADO DA BAHIA

A partir do início dos anos 2000, na Bahia, foram implementadas políticas públicas de segurança com base no videomonitoramento por Circuito Fechado de Televisão (CFTV), através de instalação de câmeras de vigilância na cidade de Salvador, especificamente no circuito do Carnaval, orla e centro da cidade, como medida de prevenção e repressão criminal (FREITAS FILHO, 2018). Essa ação se baseou no estímulo à inovação tecnológica e utilização das TICs, previsto no PNS/2000, imputando a necessidade de o Estado brasileiro desenvolver novas ações preventivas e de combate à criminalidade.

A partir do escopo inicial com o videomonitoramento por CFTV, muitas foram as alterações dessa política, passando pelo compartilhamento de imagens, transmissão de imagens via ondas de rádios, até a instalação de cabos de fibra ótica, na busca por mais eficiência para o sistema. No entanto, a capacitação dos policiais ainda era uma dificuldade a ser superada. A partir de 2012, o projeto de instalação de câmeras de videomonitoramento foi ampliado, primeiro em razão da possibilidade de captação de recursos do Fundo Nacional da Segurança Pública do Governo Federal e segundo pela vinda de grandes eventos esportivos para o Brasil, como a Copa das Confederações, em 2013, e a Copa do Mundo, em 2014, sendo a Bahia um dos estados-sede dos eventos.

Em 2016, foi instituído o Centro de Operações e Inteligência 2 de Julho (COI), com a finalidade de viabilizar e fortalecer a atuação integrada e transversal, bem como a coordenação das operações táticas e operacionais das forças de segurança pública. Assim, o Decreto Estadual nº 16.852/2016 (BAHIA, 2016) estabeleceu o fortalecimento e integração das forças de segurança pública e defesa civil, com recursos tecnológicos, para tomadas de decisões conjuntas, bem como o uso de equipamentos tecnológicos de última geração capazes de capturar uma imagem fiel e em tempo real. Foi também definida a utilização de solução integradora capaz de aglutinar sistemas de informação, comunicação e videomonitoramento, viabilizando a interoperabilidade do sistema (BAHIA, 2016).

O legado dos equipamentos adquiridos e os programas de segurança pública desenvolvidos na Bahia para as copas, além do Decreto nº 16.852/2016, atuaram como precursores dos projetos seguintes. Assim, em 2018, quando o PNS/2018 possibilitou a utilização do RF, a Bahia o aplicou, via IA, como política pública de segurança. Foi então implementado o Projeto Vídeo Policiamento – Mais Inteligência na Segurança, com o escopo de implantar ferramentas de pesquisas de registros, traçar trajetórias de pessoas ou veículos enquadrados ou não como suspeitos, bem como realizar análise situacional de trechos de gravação das câmeras, com o objetivo de subsidiar as ações do Centro de Operações de Inteligência (COI).

Destaca-se que a utilização do RF pela Secretaria de Segurança Pública da Bahia (SSP-BA) extrapolou os limites previstos na PNS/2018, visto que as câmeras de videomonitoramento por RF não foram instaladas para fins de fiscalização de fronteiras e apenas em locais citados no referido documento, mas também em ruas do circuito do carnaval, orla e centro da cidade de Salvador sem existir qualquer aparato legislativo, ainda que estadual, que permitisse essa utilização da RF por IA para fins de segurança pública.

Outro fato que de destaca é que o RF, via IA, não foi inicialmente previsto no escopo da Licitação e do Contrato nº 002/2014/DG/SSP-RDC1, vencida pelo Consórcio Projeto Cige Bahia, cujo objeto foi o videomonitoramento. A inclusão do RF, via IA, ocorreu mediante aditivo contratual em que foi escolhida a empresa chinesa Huawei para fornecimento da referida tecnologia, sem que esta empresa tivesse participado anteriormente de qualquer fase da licitação, sob a justificativa da empresa ser líder global da solução tecnológica.

O aditivo contratual apresentou, como uma das entregas, a solução de análise de vídeo avançada, com a aplicação de técnicas de RF, de reconhecimento das placas de veículos e técnicas de analise comportamental e situacional, que são técnicas de utilização invasivas do ser humano, através da análise de sua biometria facial, sendo que a forma indiscriminada de uso da tecnologia e, principalmente, a análise comportamental e situacional poderia implicar clara violação da privacidade e da proteção de dados pessoais, como afirma Rodotà (2004), ao dispor sobre o perigo da utilização dessa tecnologia que poderia investigar o estado da alma das pessoas.

É importante destacar que a escolha da Huawei e a implementação do RF por IA na Bahia, em 2018, não foi precedida de mecanismos de participação popular, a exemplo de audiências e consultas públicas, participação de entes da sociedade civil, ou ainda do Ministério Público. Ante questionamento feito à Ouvidoria Geral do Estado da Bahia

quanto à referida participação popular, a resposta foi lacônica ao afirmar que o projeto era piloto e que os resultados já se mostravam exitosos.

A partir do ano de 2019, a utilização do RF, via IA, foi ampliada, com o projeto Vídeo-Polícia Expansão, mediante um aumento exponencial das instalações de câmeras de RF para Salvador e o interior da Bahia, com perspectiva de implantação em 80 municípios baianos (BAHIA, 2023). O objeto da licitação para aplicação de videomonitoramento e RF, via IA, mudou da instalação de câmeras e acessórios para a compra de serviços, o que seria uma vantagem, visto que a vencedora da licitação, a empresa Oi/Avantia, prestava serviços de cessão e instalação dos equipamentos que permitiam a operacionalização do videomonitoramento, suprindo a falta de profissionais da administração pública com especialização em tecnologias mais complexas (BAHIA, 2019a).

Para redução de riscos aos direitos fundamentais de proteção de dados pessoais, a Huawei concederia as licenças para o uso do software de RF, sem acesso aos dados pessoais biométricos captados, que seriam geridos exclusivamente pelos profissionais da SSP-BA, com restrição de acesso, sendo considerada uma medida de minimização de riscos de vazamento de dados pessoais sensíveis.

Outra forma de redução de riscos aos direitos fundamentais da liberdade, privacidade e proteção de dados pessoais apresentada no Projeto Vídeo-Polícia Expansão foi a recomendação de abordagem das pessoas reconhecidas pelo algoritmo apenas com similaridade superior a 90% (BAHIA, 2019c), ainda que a previsão do termo de referência indicasse a possibilidade de abordagem a partir de 50% de similaridade. Cumpre observar que a SSP-BA determinou que os pontos de imagem de RF não seriam aplicados para análise comportamental ou situacional, na medida em que esses dados são considerados sensíveis e poderiam desencadear violação à privacidade (BAHIA, 2019a).

Segundo a Ouvidoria Geral do Estado da Bahia, em resposta ao questionário enviado pelas autoras deste artigo, o Projeto Vídeo-Polícia Expansão utilizou mecanismos de participação popular na sua licitação para adoção do RF, a exemplo de audiência pública, documentos de avisos e resumos dos editais de publicação publicados no Diário Oficial do Estado e em jornais de grande circulação, conforme determina o artigo 54 da Lei de Licitações da Bahia, Lei nº 9.433/2005 (BAHIA, 2005). Há destaque para o fato de a licitação do projeto também ter sido supervisionada pelo Ministério Público do Estado da Bahia (MP-BA), Tribunal de Contas do Estado da Bahia (TCE-BA) e Procuradoria Geral do Estado da Bahia (PGE-BA) (BAHIA, 2021), o que demostrou a mudança legal no

processo interno de adoção do RF, conferindo mais legitimidade e publicidade na contratação da vencedora que operaria o objeto do certame.

Por sua vez, em resposta ao questionamento sobre de qual banco de dados são retiradas as informações para a realização do RF, a pesquisa encontrou dissonância de respostas. A resposta da Ouvidoria Geral do Estado da Bahia indicou que o banco de dados de mandados de prisão e desaparecidos é de fonte exclusiva da SSP-BA, e alimentada por esta. No entanto, em entrevista (G1, 2019), o então Secretário de Segurança Pública informou que as redes sociais também seriam utilizadas como banco de dados para consulta pela SSP-BA. Ao site Intercept, em 2021, o coronel Marcos Oliveira confirmou que os policias se utilizavam de imagens públicas das redes sociais para fazer investigação de algum crime (FALCÃO, 2021).

A forma de operacionalização da ferramenta, sem transparência quanto à base de dados utilizada pelo Estado da Bahia, poderá impactar o conceito de uma sociedade em que todos poderão ser reconhecidos pelo sistema, havendo uma inversão de valores sociais e supressão de direitos, uma vez que, se todos serão vistos como suspeitos e reconhecidos (SOLOVE, 2011b), poderá haver violação do princípio da presunção da inocência (FERREIRA, 2022), privacidade e proteção de dados pessoais (OLIVEIRA, 2021) e se conferirá uma ilusão de liberdade social (NEGRI; OLIVEIRA; COSTA, 2020).

Ademais, é importante considerar os possíveis desafios encontrados pelo Estado da Bahia quanto à existência de possíveis vieses raciais e sexistas nos algoritmos do RF, considerando a aplicação da ferramenta em Salvador, considerada a capital que contém mais de 81% de pessoas autodeclaradas negras ou pardas (IBGE, 2018), por ser este um público com maior incidência de erros de RF em pesquisas realizadas pelo mundo (NORRIS; ARMSTRONG, 1999; BUOLAMWINI; GEBRU, 2018).

Importante observar que, em pesquisa realizada pelo Observatório de Segurança Pública (2020), 90,5% dos presos por via do RF são pessoas pretas ou pardas no Brasil, um percentual que se reflete na maioria das prisões pelo uso do RF também na Bahia[6]. Segundo o superintendente de Gestão Tecnológica e Organizacional da SSP-BA, coronel PM Marcos Oliveira, isso ocorreria apenas por uma consequência lógica do fato de que a maioria da população da localidade se autodeclara preta ou parda (PALMA; PACHECO, 2020), o que diferiria da tese de racismo algoritmo, como defende Silva, T. (2020).

[6] Não foi possível averiguar na pesquisa o percentual exato de pessoas presas pelo uso do RF na Bahia que são pretos e pardos.

Os dados coletados através do questionário enviado à Ouvidoria Geral do Estado da Bahia indicam que, até novembro de 2021, não existiram erros no RF por IA tendo em vista o protocolo operacional utilizado pelas polícias para identificação e condução do capturado à prisão. Pesquisa realizada na imprensa, em livros, artigos científicos e sites institucionais ou em notas oficiais governamentais, sobre a existência de possíveis erros de prisão decorrentes de erro de identificação do RF, via IA, não encontrou indicação de erros, o que constitui um ponto positivo da aplicação eficiente da ferramenta, até novembro de 2021.

No que tange a possível existência de erros de abordagem de pessoas indevidamente identificadas pela ferramenta de RF, mas que não necessariamente se converteram em prisões, a resposta a esse questionamento pela Ouvidoria Geral do Estado da Bahia foi de que, até novembro de 2021, não havia conhecimento sobre erros de abordagens provocados pela indicação da ferramenta[7].

Destaca-se, entretanto, que, pela análise de percentual de abordagens de policiais no Brasil ser em números muito superiores na população negra, com a falácia das instituições de segurança pública de que os negros seriam mais propensos a cometer crimes (ALCADIPANI; BUENO; LIMA, 2021), aliado à existência comprovada de vieses raciais e sexistas nas ferramentas, não há como ser descartada a possibilidade da existência de propensão de mais erros de abordagem para a população negra na Bahia por racismo embutido no algoritmo (SILVA, T., 2020).

Sobre a possibilidade de compartilhamento dos dados biométricos com outros governos, empresas ou ainda mediante transferências internacionais, a Ouvidoria Geral do Estado da Bahia destacou que não há compartilhamento de dados sensíveis, o que minimizaria possíveis incidentes de vazamentos de dados e violação de princípios de proteção de dados pessoais.

Importante destacar que a utilização do RF pela segurança pública da Bahia é vista pela sociedade baiana de forma aceitável em sua maioria, conclusão essa inferida pela pouca oposição quanto à utilização do RF pela SSP-BA no Poder Judiciário, conforme já destacado neste artigo, ou ainda em notícias jornalísticas que versam sobre o tema. Observa-se que o Poder Judiciário da Bahia e o STJ, em que pese poucas ações, se

[7] Segundo Palma e Pacheco (2020), um possível erro de abordagem ocorreu em setembro de 2019, quando o RF teria errado ao identificar um assaltante procurado com um jovem negro de 25 anos e que tinha deficiência mental.

posicionaram pela legalidade da aplicação do RF por IA como política pública, ainda que não haja regulação específica para utilização no Brasil.

CONSIDERAÇÕES FINAIS

O presente trabalho objetivou descrever os benefícios e desafios da utilização da tecnologia do RF como política de segurança pública pelo Estado da Bahia frente às garantias e desenvolvimento dos direitos fundamentais da liberdade, privacidade e proteção de dados pessoais, com destaque para os projetos Vídeo Policiamento – Mais Inteligência na Segurança e Vídeo-Polícia Expansão.

Constatou-se que, no Brasil, o estímulo à formulação e implementação de políticas públicas na área de segurança, envolvendo tecnologia, ocorreu com o PNS/2000, sendo que houve um maior estímulo ao uso de tecnologias com os editais de financiamentos públicos, a partir de 2012. Em 2018, com o PNS/2018, houve a primeira menção ao RF, via IA, para fiscalização de fronteiras, portos e aeroportos, sendo o Estado da Bahia pioneiro na sua utilização com política de segurança pública, com os projetos Vídeo Policiamento – Mais Inteligência na Segurança e Vídeo-Polícia Expansão, implementados em 2018 e 2019, respectivamente.

A pesquisa que embasa este artigo demonstrou os principais benefícios e riscos da implementação da política pública realizada pela SSP-BA. Foram identificados pontos positivos quanto à eficiência e ao custo-benefício, mão de obra qualificada e especializada em tecnologias complexas, chamados de atendimento, privilegiando o princípio da universalidade e celeridade, além da inexistência de erros quanto ao reconhecimento de pessoas, até novembro de 2021, quando tinham sido capturadas 282 pessoas foragidas ou procuradas pela Justiça.

Outros pontos positivos também chamaram atenção: o cumprimento de direitos fundamentais, a exemplo da não utilização do RF para análise situacional ou comportamental das pessoas; utilização de expansão de mecanismos prévios de participação popular como audiências públicas e envolvimento de órgãos de controle como o TCE-BA, MP-BA e PGE-BA, pelo projeto Vídeo-Polícia Expansão; não compartilhamento de dados sensíveis biométricos com entidades privadas ou transferência internacional; existência de controles de acesso aos dados; *cloud* (nuvem) privada e preocupação com a segurança do Centro de Controle de Operações onde se localiza o *data center* com os dados armazenados.

Destaca-se, positivamente ainda, a informação quanto à existência de protocolo interno nas polícias da Bahia limitando a abordagem a pessoas reconhecidas pelo RF com similaridades acima de 90%, o que reduziria chances de erros no RF – o que foi feito mesmo havendo no Termo de Referência da licitação do projeto Vídeo-Polícia Expansão a possibilidade de a abordagem poder ser realizada em caso de similaridades acima de 50%.

Por outro lado, identificaram-se riscos aos direitos fundamentais da liberdade, privacidade e proteção de dados pessoais quando da operacionalização da referida política, com destaque para a falta de uma regulamentação legal específica e para a inclusão do RF, via IA, como aditivo a um contrato de licitação que seria para aquisição de câmeras de videomonitoramento por CFTV, mediante a escolha da empresa Huawei para operacionalização das licenças do software de RF, simplesmente sob a justificativa de que a empresa possuía *know how* para a prestação de serviços.

Ainda, a pesquisa demonstrou que não foram realizadas previamente audiências públicas e debates com a sociedade civil e órgãos de controle do Estado quanto à inserção do RF, por IA, na segurança pública do Estado da Bahia no projeto pioneiro do Vídeo Policiamento – Mais Inteligência na Segurança, em 2018, apesar de ser uma ferramenta de alto risco ao direitos fundamentais das pessoas.

De acordo com os dados coletados, constatou-se que falta transparência nos dados oficiais apresentados para a operacionalização da política pública, principalmente quando de sua entrada em 2018 no Estado, de forma a comprometer uma avaliação mais completa – por exemplo, quando há divergências nas respostas sobre quais bancos de dados são utilizados para consulta pela SSP-BA. Esse questionamento se torna importante porque uma política pública que envolve riscos a direitos fundamentais deverá ter limitações no seu uso, de forma a se tornar uma exceção, diferentemente do objetivo do governo da Bahia de difundir o RF para mais de 15 milhões de pessoas.

Por fim, ressaltam-se os riscos identificados de estímulo ao encarceramento como suposta segurança; possibilidade de incidentes de vazamentos de dados pessoais; difusão do *chilling effect* de forma a inibir as pessoas a irem para áreas públicas monitoradas; riscos de danos físicos ao prédio onde se localiza o *data center* e de haver perdas de dados pessoais já armazenados. Além de falta de transparência quanto aos locais do videomonitoramento e temporalidade do armazenamento dos dados, o que pode implicar violação ao princípio de minimização previsto na LGPD.

A partir das análises realizadas, é possível identificar melhorias na implementação da política pública, no que se refere à observância dos princípios constitucionais da liberdade, privacidade e proteção de dados pessoais, de forma que esta seja planejada e executada com *Privacy by Desing* (privacidade como padrão), transparência, conceitos éticos, limites, finalidade específica, prestação de contas – *accountability*, proporcionalidade e não discriminação. Deve ser implementada, também, a previsão de planos de incidentes de vazamento de dados e e devem ser elaborados relatórios técnicos periódicos que apresentem mais dados sobre os resultados da política ao público. Destaca-se a possibilidade de uma regulação legal específica constituir na compatibilização da política com os direitos fundamentais na sua aplicação.

O estudo possui limitações, a exemplo da escassez de divulgação de dados institucionais oficiais, por ser uma política pública recente e porque questões relativas à segurança pública sofrem restrições de confidencialidade e sigilo; não analisou os impactos da política antes e depois da sua implementação, assim como não utilizou análises do Relatório da Comissão de Juristas do Senado Federal que regula a IA no Brasil e que pode trazer conclusões que impactam na aplicação da política, seja em sua regulação, moratória ou até banimento. Espera-se, com esse estudo abrir oportunidades para estudos posteriores, principalmente pela complexidade e sensibilidade que envolve políticas públicas de segurança, eficiência operacional, inovação e direitos fundamentais.

REFERÊNCIAS

ALBARDEIRO, N. M. E. (2020). **Body-Worn Cameras**: Perceção dos polícias com funções operacionais da Divisão Policial da Amadora. 2020. 98 f. Dissertação (Mestrado) – Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/32969/1/156427_Albardeiro_Body-Worn%20Cameras-Perce%c3%a7%c3%a3o%20dos%20Pol%c3%adcias%20com%20fun%c3%a7%c3%b5es%20operacionais%20da%20Divis%c3%a3o%20Policial%20.pdf. Acesso em: 03 abr. 2022.

ALCADIPANI, R. (2020). Novas tecnologias e a criminalidade: o crime do futuro e a polícia do passado. **Estadão**, São Paulo, 14 jan. Disponível em: https://politica.estadao.com.br/blogs/gestao-politica-e-sociedade/novas-tecnologias-e-a-criminalidade-o-crime-do-futuro-e-a-policia-do-passado/. Acesso em: 03 abr. 2022.

ALCADIPANI, R.; BUENO, S.; LIMA, R. S. (2021). Evolução das mortes violentas intencionais no Brasil. *In*: FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Anuário Brasileiro de Segurança Pública 2021**, [São Paulo], ano15. ISSN 1983-7364.

ARANHA, E.; FERREIRA, L. M. T. (2020). O direito fundamental à proteção de dados e a importância da proposta de alteração constitucional nº 17/2019. **OAB-RJ**, Rio de Janeiro,

27 jan. Disponível em: https://www.oabrj.org.br/noticias/artigo-direito-fundamental-protecao-dados-importancia-proposta-alteracao-constitucional. Acesso em: 10 abr. 2022.

BAHIA. (2005). Lei nº 9.433, de 01 de março de 2005. Dispõe sobre as licitações e contratos administrativos pertinentes a obras, serviços, compras, alienações e locações no âmbito dos poderes do Estado da Bahia e dá outras providências. **Diário Oficial do Estado (DOE)**, Bahia, 02 mar. 2005. Disponível em: https://leisestaduais.com.br/ba/lei-ordinaria-n-9433-2005-bahia-dispoe-sobre-as-licitacoes-e-contratos-administrativos-pertinentes-a-obras-servicos-compras-alienacoes-e-locacoes-no-ambito-dos-poderes-do-estado-da-bahia-e-da-outras-providencias. Acesso em: 05 abril 2021.

BAHIA. (2016). Decreto nº 16.852, de 14 de julho de 2016. Institui o Centro de Operações e Inteligência e o Comitê de Gestão de Crises, no âmbito da Secretaria da Segurança Pública. **Casa Civil**, Salvador. Disponível em: http://www.legislabahia.ba.gov.br/documentos/decreto-no-16852-de-14-de-julho-de-2016. Acesso em: 12 maio 2022.

BAHIA. (2019a). Secretaria de Segurança Pública. **Termo de Referência:** Projeto Vídeo-Polícia Expansão. Salvador, 14 maio 2019. Disponível em: https://comprasnet.ba.gov.br/sites/default/files/termo_de_referencia_v1.pdf. Acesso em: 03 abr. 2021.

BAHIA. (2019b). Secretaria de Segurança Pública. **Reconhecimento Facial estará nos portais e em outros locais**. Salvador, 26 fev. 2019. Disponível em: http://www.ssp.ba.gov.br/2019/02/5252/Reconhecimento-Facial-estara-nos-portais-e-em-outros-locais-.html. Acesso em: 03 abr. 2021.

BAHIA. (2019c). Secretaria de Segurança Pública. **Reconhecimento facial impede entrada de homicida em circuito**. Salvador, 05 mar. 2019. Disponível em: https://www.ssp.ba.gov.br/2019/03/5310/Reconhecimento-facial-impede-entrada-de-homicida-em-circuito-.html. Acesso em: 03 abr. 2021.

BAHIA (2021). Secretaria de Segurança Pública. **Governador autoriza expansão de tecnologia a mais 77 cidades baianas**. Salvador, 27 jul. 2021. Disponível em: https://www.ssp.ba.gov.br/2021/07/10138/Governador-autoriza-expansao-de-tecnologia-a-mais-77-cidades-baianas.html. Acesso em: 03 fev. 2022.

BAHIA. (2023). **O Portal Oficial do Estado da Bahia**. Salvador. Disponível em: https://www.bahia.ba.gov.br/2023/07/noticias/seguranca/total-de-326-presos-pelo-reconhecimento-facial-e-queda-de-mortes-violentas-sao-destaques-no-primeiro-semestre-de-2023-na-bahia/. Acesso em: 03 ago. 2023.

BARBOSA, A. D. (2018). **Segurança, Biopolítica e Educação: o empresariamento da segurança pública como dispositivo pedagógico**. 200 f. Tese (Doutorado em Educação), Universidade Federal da Ceará, Fortaleza, 2018.

BIONI, B. R. (2018). **Proteção de Dados Pessoais:** A Função e os Limites do Consentimento. Rio de Janeiro: Forense.

BLUM, R. O.; LOPEZ, N. (2020). Lei Geral de Proteção de Dados no setor público: transparência e fortalecimento do Estado Democrático de Direito. **Cadernos Jurídicos da Escola Paulista de Magistratura**, São Paulo, ano 21, n. 53, p. 171-177, jan./mar.

BRASIL.(1988). **Constituição da República Federativa do Brasil**. Brasília: Senado.

BRASIL. (2000). Ministério de Segurança Pública. Plano Nacional de Segurança Pública.

BRASIL. (2010). Lei nº 12.258, de 15 de junho de 2010. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal), e a Lei no 7.210, de 11 de julho de 1984 (Lei de Execução Penal), para prever a possibilidade de utilização de equipamento de vigilância indireta pelo condenado nos casos em que especifica. **Diário Oficial da União**, Brasília, DF, 16 jun. 2010. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/lei/l12258.htm#:~:text=L12258&text=LEI%20N%C2%BA%2012.258%2C%20DE%2015%20DE%20JUNHO%20DE%202010.&text=Altera%20o%20Decreto%2DLei%20n,nos%20casos%20em%20que%20especifica.Acesso em: 02 mar. 2021.

BRASIL. (2012). Lei nº 12.681, de 04 de julho de 2012. Institui o Sistema Nacional de Informações de Segurança Pública, Prisionais e sobre Drogas - SINESP; altera as Leis nº s 10.201, de 14 de fevereiro de 2001, e 11.530, de 24 de outubro de 2007, a Lei Complementar nº 79, de 7 de janeiro de 1994, e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 - Código de Processo Penal; e revoga dispositivo da Lei nº 10.201, de 14 de fevereiro de 2001. **Diário Oficial da União. Brasília**, 29 jun. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12681.htm. Acesso em: 02 mar. 2021.

BRASIL. (2014). Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 02 mar. 2021.

BRASIL.(2018a). Ministério da Segurança Pública. **Plano Nacional de Segurança Pública e Defesa Social 2018-2028**. Disponível em: https://cispregional.mpba.mp.br/wp-content/uploads/2020/04/11.-Plano-Nacional-de-Seguran%C3%A7a-P%C3%BAblica-2018-compactado.pdf. Acesso em: 20 dez. 2020.

BRASIL. (2018b). Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 ago. 2021.

BRASIL. (2021). Ministério da Justiça e Segurança Pública. **Plano Nacional de Segurança Pública e Defesa Social 2021-2030**. [S.L.]. Disponível em: https://www.gov.br/mj/pt-br/acesso-a-informacao/acoes-e-programas/susp/PNSP%202021-2030. Acesso em: 20 fev. 2022.

BRASIL. (2022). Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial da União**. Brasília, DF, 2022c. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 11 fev. 2022.

BUOLAMWINI, J. A.; GEBRU, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research. **Massachussets Institute of Technology**. Disponível em: http://gendershades.org/overview.html?utm_campaign=newsletterIdEA&utm_medium=email&utm_source=Revue%20newsletter. Acesso em: 01 set. 2020.

CANCELIER, M. V. L. (2017). O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro. **Sequência**, Florianópolis, n. 76, p. 213-240, ago. Disponível em: https://www.scielo.br/j/seq/a/ZNmgSYVR8kfvZGYWW7g6nJD/?format=pdf&lang=pt. Acesso em: 03 ago. 2021.

CARVALHO, V. A.; SILVA, M. R. F. (2011.). Política de Segurança Pública no Brasil: avanços, limites e desafios. **R. Katál**, Florianópilis, v. 14, n. 1, p. 59067, jan./jun, 2011.

DONEDA, D. (2006). **Da privacidade à proteção dos dados pessoais**. Rio de Janeiro: Renovar.

DRUMMOND, M.; CARNEIRO, J. V. (2022). Panorama Regulatório da Inteligência Artificial no Brasil. **ITS**. Rio de Janeiro. Disponível em: https://itsrio.org/wp-content/uploads/2022/04/Relatorio-Panorama-IA.pdf. Acesso em: 28 jun. 2022.

DUARTE, D. E. (2022). Câmeras corporais e a ação policial: As condições de emergência e os impactos dos dispositivos de controle em São Paulo. **NEV**, São Paulo. Disponível em: https://nev.prp.usp.br/noticias/cameras-corporais-e-acao-policial-as-condicoes-de-emergencia-e-os-impactos-dos-dispositivos-de-controle-em-sao-paulo/. Acesso em: 01 jun. 2022.

FALCÃO, C. (2021). Rui Costa está transformando a Bahia em um laboratório de vigilância com reconhecimento facial. **The Intercept**, [S.L.], 20 set. Disponível em: https://theintercept.com/2021/09/20/rui-costa-esta-transformando-a-bahia-em-um-laboratorio-de-vigilancia-com-reconhecimento-facial/. Acesso em: 03/04/2022.

FERREIRA, G. (2022). Reconhecimento Facial: considerações sobre o banimento desta tecnologia na segurança. **YouTube**, 2022. Disponível em: https://www.youtube.com/watch?v=2uJlbZnVqK4&t=650s. Acesso em: 12 jun. 2022.

FREITAS FILHO, N. B. (2018). O videomonitoramento nas tecnologias de comunicação na Secretaria de Segurança Pública do Estado da Bahia. *In*: MAGALHÃES, A. C. S.; JESUS, A. R. (Org.). **Telecomunicações na Segurança Pública do Estado da Bahia:** Do sino à era digital. Biblioteca Digital COGER, Salvador. Disponível em: https://bibliotecacoger.ssp.ba.gov.br/. Acesso em: 03 maio 2022.

G1. (2019). **Monitor da Violência:** assassinatos caem em 2019, mas letalidade policial aumenta; nº de presos provisórios volta a crescer. [S.L.], 16 dez. Disponível em: https://g1.globo.com/retrospectiva/2019/noticia/2019/12/16/monitor-da-violencia-assassinatos-caem-em-2019-mas-letalidade-policial-aumenta-no-de-presos-provisorios-volta-a-crescer.ghtml. Acesso em: 12 maio 2021.

IBGE. (2018). **Pesquisa Nacional por Amostra de Domicílio Contínua Anual - PNAD:** Microdados 2018. Rio de janeiro: IBGE. Disponível em: ftp://ftp.ibge.gov.br/Trabalho_e_Rendimento/Pesquisa_Nacional_por_Amostra_de_Domicilios_continua/Anual/Microdados/Dados/. Acesso em: 09 set. 2021.

IPEA. (2023). **Atlas da Violência**. Disponível em: //www.ipea.gov.br/atlasviolencia/dados-series/328. Acesso em: 01 ago. 2023.

JOÃO, D. O.; LUNARDO, G. M.; CRISTIANO, S. M. A. (2016). Políticas de Segurança Pública e direitos humanos em Santa Catarina. *In*: SPANHOL, J. F. (Org.). **Tecnologia e Informação na Segurança Pública e Direitos Humanos**. v. 2. São Paulo: Editora Edgar Blucher .

KARAM, M. L (, jan. 2007). Monitoramento eletrônico: a sociedade do controle. **Boletim do Instituto Brasileiro de Ciências Criminais**, São Paulo, ano 14, n. 170, p. 4-5.

LOPES, E. S. (2009). **Política e segurança pública:** uma vontade de sujeição. Rio de Janeiro: Contraponto.

MARCINEIRO, N. P.; GIOVANNI, C. (2005). **Polícia Comunitária**: Evoluindo para a polícia do século XXI. Florianópolis: Insular.

NEGRI, S. M. C. A.; OLIVEIRA, S. R.; COSTA, R. S. (2020). O uso da tecnologia de reconhecimento facial baseadas em inteligência artificial e à proteção de dados. **Revista de Direito Público**, Brasília, v. 17, n. 93, p. 82-103, mai/jun.

NOBLE, S. (2018). Algorithms of oppression: How search engines reinforce. **YouTube**. Disponível em: https://www.youtube.com/watch?v=oqelqdDIDSs. Acesso em: 03 fev. 2022.

NORRIS, C.; ARMSTRONG, G. (1999). **The Maximun Surveillence Society**. The Rise of CCTV. Oxford: Berg.

OBSERVATÓRIO DE SEGURANÇA PÚBLICA. (2020). Site sobre segurança pública. Marília, SP. Disponível em: https://www.observatoriodeseguranca.org/a-seguranca-publica-no-brasil/#tab-polticasdeseguranapblica. Acesso em: 10 mar. 2022.

OLIVEIRA. S. R. Sorria você está sendo filmado. Repensando Direitos na Era do Reconhecimento Facial. **Revista dos Tribunais**. São Paulo. 2021.

PALMA, A.; PACHECO, C. (2020). Entenda como funciona o reconhecimento facial que ajudou a prender mais de 100 na BA. **Correio 24 horas**, Salvador, 05 jan. Disponível em: https://www.correio24horas.com.br/noticia/nid/entenda-como-funciona-o-reconhecimento-facial-que-ajudou-a-prender-mais-de-100-na-ba/. Acesso em: 24 ago. 2020.

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

RODOTÀ, S. (2004). Transformações do Corpo. **Revista Trimestral de Direito Civil**, v. 19, n. 5, p. 91-115.

RUBACK, L.; AVILA, S.; CANTERO, L. (2021). Vieses no Aprendizado de Máquina e suas Implicações Sociais: Um Estudo de Caso no Reconhecimento Facial. **Biblioteca Digital da Sociedade Brasileira de Computação**, Porto Alegre. Disponível em: https://sol.sbc.org.br/index.php/wics/article/view/15967/15808. Acesso em: 04 nov. 2021.

SANTOS, A. S.; LIMA, E. G.; SOUZA, W. B. (2020). **Tecnologia da Informação na Segurança Pública**: a necessidade de criação de uma base nacional de dados de registro de ocorrência e atendimentos de emergência. 24 p. Trabalho de Conclusão de Curso – Polícia Militar do Estado de Rondônia, Centro de Aperfeiçoamento de Oficiais, Porto Velho, 2020. Disponível em: https://dspace.mj.gov.br/bitstream/1/4606/1/Tecnologia%20da%20Informa%C3%A7%C3%A3o%20na%20Seguran%C3%A7a%20P%C3%BAblica_A%20necessidade%20de%20cria%C3%A7%C3%A3o%20de%20uma%20Base%20Nacional%20de%20Dados%20de%20Registro%20de%20Ocorr%C3%AAncia%20e%20Atendimento%20de%20Emerg%C3%AAncia.pdf . Acesso em: 04 maio 2022.

SILVA JUNIOR, J. J. (2020). **Redes neurais profundas para reconhecimento facial no contexto de segurança pública**. 85 f. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Goiás, Goiânia, 2020.

SILVA, J. A. (2008). **Curso de Direito Constitucional Positivo**. 30. ed. São Paulo: Malheiros.

SILVA, P. G. F. da. (2020). Sorria você está sendo reconhecido: o reconhecimento facial como violador de direito humanos? **ITS Rio**, Rio de Janeiro, 26 ago. Disponível em: https://feed.itsrio.org/sorria-voc%C3%AA-est%C3%A1-sendo-reconhecido-o-reconhecimento-facial-como-violador-de-direitos-humanos-4113914441d3. Acesso em: 02 fev. 2022.

SILVA, S. P. (2020). Democracia, inteligência artificial e desafios regulatórios: Direitos, dilemas e poder nas sociedades datificadas. **E-legis**, Brasília, DF, n. 33, p. 226-248, set./dez. ISSN: 2175.0688.

SILVA, T. (2020). Racismo Algorítmico em Plataformas Digitais: microagressões e discriminação em código. *In*: SILVA, T. (Org.). **Comunidades, Algoritmos e Ativismo Digitais**: olhares afrodiaspóricos. São Paulo: Literarua.

SOLOVE, D. J. (2011a). **Nothing to Hide**: The false Tradeoff between Privacy and Security. New Haven: Yale University Press.

SOLOVE. (2011b). **Why Privacy Matters Even if you have 'Nothing to Hide'**. The Chronicle of higher education.

VARGAS, E. N. P.; RIBEIRO, M. M. (2023). A Sociedade do Controle Digital e a Segurança Pública Brasileira. **Revista Direito Unifacs**: Debate Virtual, n. 277, jul.

VARGAS, E. N. P.; RIBEIRO, M. M. (2020). Desafios da Administração Pública no controle e proteção dos dados sensíveis: o sistema Datavalid. *In*: JESUS, D. M. *et al.* (Org.). **Ciências Sociais aplicadas III**: Diálogos Contemporâneos. Salvador: Mente Aberta. p. 327-339.

VIDAL, E. L. (2014). **Monitoramento Eletrônico: Aspectos Teóricos e Práticos**. 106 f. Dissertação (Mestrado) – Universidade Federal da Bahia, Salvador, 2014. Disponível em: https://repositorio.ufba.br/bitstream/ri/17989/1/Disserta%c3%a7%c3%a3o%20final%20-%20Eduarda%20de%20Lima%20Vidal.pdf. Acesso em: 03 abr. 2021.

WERTHEIN, J. (2000). A Sociedade da Informação e seus desafios. **Ci. Inf.**, Brasília, v. 29, n. 2, p. 71-77, maio/ago.

Érica Nascimento Pinheiro Vargas

Mestre e especialista em Direito, Governança e Políticas Públicas e professora de Direito Digital no Curso de Especialização em Mídias Sociais do Centro Universitário Jorge Amado.

Mônica Matos Ribeiro

Doutora e mestra em Administração, professora da Universidade do Estado da Bahia (Uneb) e do mestrado profissional em Direito, Governança e Políticas Públicas da Universidade Salvador (Unifacs).