MESTRADO PROFISSIONAL INTERDISCIPLINAR EM DIREITO, GOVERNANÇA E POLÍTICAS PÚBLICAS

ÉRICA NASCIMENTO PINHEIRO VARGAS

O USO DA TECNOLOGIA DE RECONHECIMENTO FACIAL COMO POLÍTICA DE SEGURANÇA PÚBLICA NO ESTADO DA BAHIA

Salvador
2022

ÉRICA NASCIMENTO PINHEIRO VARGAS

O USO DA TECNOLOGIA DE RECONHECIMENTO FACIAL COMO POLÍTICA DE SEGURANÇA PÚBLICA NO ESTADO DA BAHIA

Dissertação apresentada ao Programa de Pós-Graduação em Direito, Governança e Políticas Públicas da Universidade Salvador – Unifacs como requisito parcial para obtenção do título de Mestra em Direito, Governança e Políticas Públicas.

Orientadora: Profª. Drª. Mônica Matos Ribeiro.

Salvador
2022

Ficha Catalográfica elaborada pelo Sistema de Bibliotecas da Universidade Salvador UNIFACS.

Vargas, Érica Nascimento Pinheiro

O uso da tecnologia de reconhecimento facial como política de segurança pública no Estado da Bahia. / Érica Nascimento Pinheiro Vargas. – Salvador: UNIFACS, 2022.

176 f.: il.

Dissertação apresentada ao Programa de Pós-Graduação em Direito, Governança e Políticas Públicas da Universidade Salvador – Unifacs como requisito parcial para obtenção do título de Mestra em Direito, Governança e Políticas Públicas.

Orientadora: Profª. Drª. Mônica Matos Ribeiro.

1. Direito. 2. Políticas Públicas – Salvador-BA. 3. Tecnologia da Informação e Comunicação. 4. Videomonitoramento. Reconhecimento facial. I. Ribeiro, Mônica Matos, orient. II. Título.

CDD: 340

ÉRICA NASCIMENTO PINHEIRO VARGAS

O USO DA TECNOLOGIA DE RECONHECIMENTO FACIAL COMO POLÍTICA DE SEGURANÇA PÚBLICA NO ESTADO DA BAHIA

Dissertação apresentada ao Programa de Pós-Graduação Mestrado em Direito, Governança e Políticas Públicas da UNIFACS – Universidade Salvador, como requisito parcial para obtenção do título de Mestre e aprovada pela seguinte banca examinadora:

Mônica Matos Ribeiro – Orientadora _____
Doutora em Administração pela Universidade Federal da Bahia – UFBA
Universidade Salvador - Unifacs

José Vaner do Prado _____
Doutor em Desenvolvimento Regional e Urbano pela Universidade Salvador – Unifacs
Universidade Salvador - Unifacs

Ana Karine Loula Torres Rocha _____
Doutora em Educação e Contemporaneidade pela Universidade do Estado da Bahia - UNEB
Universidade Estadual da Bahia – UNEB

Salvador, ____ de _____ de 2022.

Dedico este trabalho à minha família, pelo apoio incondicional.

AGRADECIMENTOS

Agradeço a Deus por ter proporcionado conquistar esse objetivo tão sonhado e batalhado de concluir o Mestrado em Direito, Governança e Políticas Públicas.

Agradeço a minha filha Valentina, pelo amor incondicional, por me ensinar a ser mãe e por me fazer tentar ser uma pessoa melhor a cada dia, para fazê-la se orgulhar de mim.

Agradeço aos meus pais João e Maria das Graças, por terem sempre me incentivado a gostar dos estudos e querer ir além, pelo exemplo de pais que são, pela sabedoria de cada palavra e por me ensinarem o amor, a importância da família e o poder da resiliência e da fé.

Agradeço as minhas irmãs Natali e Iris, pelo amor e carinho e por estarem sempre comigo e com minha filha, acreditando na persecução de meus objetivos, em tantas vezes em que eu mesmo duvidei que iria conseguir atingi-los.

Agradeço ao meu esposo Jortan, por entender meus momentos de ausência em razão da pesquisa e pelas palavras de amor e incentivo ao meu trabalho.

Agradeço à professora Mônica, minha orientadora querida, que gentilmente me transmitiu conhecimentos e foi tão compreensiva em muitos momentos de dificuldades na continuidade da pesquisa e ao querido professor Vaner, pelo carinho e ensinamentos.

Agradeço aos meus colegas do curso de mestrado por dividir comigo tantos momentos de aprendizado e à TV Bahia e aos colegas de trabalho pelo incentivo aos estudos.

Agradeço a minha família, tios, primos e aos meus amigos e por me proporcionarem momentos de alegria.

Agradeço, *in memorian*, as pessoas que iniciaram presentes em minha vida nessa jornada do mestrado, mas que foram ao encontro da luz recentemente: a amada vovó Marina, minha inspiração de mulher forte, pilar, matriarca da família Nascimento, por cada conselho, sorriso e palavras de incentivo, pelo brilho nos olhos quando eu publicava um artigo, fazia uma *live* em que ela fazia questão de me prestigiar; aos queridos tios Josaphat (Abá) e Zequinha, Raquel, minha prima, pelo carinho e a minha amada tia Valdir, pelo amor, por me tratar como sua filha, ter acreditado no meu sonho de menina do interior de vir estudar na capital e se orgulhar de cada conquista minha ao longo dos anos e, por fim, ao colega de Mestrado Gomes, que deixará seu legado de sapiência e dedicação a educação.

“A criação bem-sucedida da inteligência artificial seria o maior evento na história da humanidade. Infelizmente, pode também ser o último, a menos que aprendamos a evitar os riscos.”

Stephen Hawking

RESUMO

A sociedade hodierna se destaca pelo avanço da tecnologia e mudanças na forma da interrelação homem/máquina, principalmente, após a criação da inteligência artificial e sua aplicação em diversos setores da sociedade, com destaque, neste estudo, para a utilização do reconhecimento facial automatizado como política de segurança pública. Nesse sentido, o objetivo desta pesquisa foi analisar 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, visando apresentar e discutir os projetos Vídeo Policiamento – Mais Inteligência na Segurança; Vídeo-Polícia Expansão e PRODETUR Salvador. O estudo partiu do pressuposto da necessidade de mais acuidade na aplicação do reconhecimento facial, via inteligência artificial, para utilização como política pública de segurança, a fim de evitar possíveis violações de direitos fundamentais das pessoas. Nesse cenário, buscou-se descrever a evolução da sociedade e o impacto das tecnologias de informação e comunicação nas políticas públicas, a partir da aplicação das tecnologias de inteligência artificial, particularmente as de reconhecimento facial, tendo como lócus privilegiado do estudo, a política pública de utilização da tecnologia de inteligência artificial, por reconhecimento facial, aplicada pela Secretaria de Segurança Pública do Estado da Bahia. Optou-se por realizar uma pesquisa qualitativa, utilizando-se o método dedutivo, de natureza exploratória, como abordagem um estudo de caso e adotou-se a técnica de análise documental. As categorias de análise utilizadas foram tecnologias da informação e comunicação, inteligência artificial, reconhecimento facial, políticas públicas de segurança e direitos fundamentais. Como resultado da pesquisa observou-se vantagens da política pública pesquisada, como ser menos letal para os policiais e pessoas abordadas, celeridade no reconhecimento de pessoas desaparecidas e foragidas da justiça e não existência de prisões eivadas de erros de reconhecimento facial na Bahia até a data de corte da pesquisa. 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 Estado da Bahia e ausência de regulamentação legal específica no Brasil sobre a referida política pública. Ainda, foram realizadas proposições de melhorias na aplicação da política, como a adoção do *Privacy by Desing*, Princípio da Precaução, Relatório de Impacto à Proteção de Dados Pessoais, transparência e prestação de contas.

Palavras-chave: Tecnologia da informação e comunicação, política pública, videomonitoramento, reconhecimento facial, segurança pública.

ABSTRACT

Today's society stands out for the advancement of technology and changes in the form of the man/machine interrelationship, especially after the creation of artificial intelligence and its application in various sectors of society, especially in this study, for the use of automated facial recognition. as a public security policy. In this sense, the objective of this research was to analyze the main benefits and risks of the implementation of the public policy of facial recognition, via artificial intelligence, applied by the Secretary of Public Security in the State of Bahia, aiming to present and discuss the Video Policing – Mais Inteligência na Safety; Video-Police Expansion and PRODETUR Salvador. The study started from the assumption of the need for more acuity in the application of facial recognition, via artificial intelligence, for use as a public security policy, in order to avoid possible violations of people's fundamental rights. In this scenario, we sought to describe the evolution of society and the impact of information and communication technologies on public policies, from the application of artificial intelligence technologies, particularly those of facial recognition, with public policy as the privileged locus of the study. use of artificial intelligence technology, by facial recognition, applied by the Secretary of Public Security of the State of Bahia. We chose to carry out a qualitative research, using the deductive method, of an exploratory nature, and as an approach a case study and the document analysis technique was adopted. The analysis categories used were information and communication technologies, artificial intelligence, facial recognition, public security policies and fundamental rights. As a result of the research, advantages of the researched public policy were observed, such as being less lethal to police officers and people approached, speed in the recognition of missing people and those who are out of justice and the lack of prisons riddled with facial recognition errors in Bahia to date. search cutoff. On the other hand, possible risks of violation of freedom, privacy and protection of personal data were also demonstrated, due to the lack of transparency in the data released by the State of Bahia and the absence of specific legal regulations in Brazil on the aforementioned public policy. Furthermore, proposals were made to improve the application of the policy, such as the adoption of Privacy by Design, the Precautionary Principle, the Impact Report on the Protection of Personal Data , transparency and accountability.

Keywords: Information and communication technology, public policy, video monitoring, facial recognition, public security.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE FLUXOGRAMAS

LISTAS DE ABREVIATURAS E SIGLAS

3D	Terceira Dimensão
ABIN	Associação Brasileira de Inteligência
ACADELPOL	Academia de Polícia Civil
ACLU	União Americana pelas Liberdades Civis
ADIN	Ação Direta de Inconstitucionalidade
ANPD	Autoridade Nacional de Proteção de Dados
ARPANET	Advanced Research Projects Agency Network
BID	Banco Interamericano de Desenvolvimento
BNMP	Banco Nacional de Monitoramento de Prisões
CAB	Centro Administrativo da Bahia
CENTEL	Central de Telecomunicações
CEO	*Chief Executive Officer*
CF	Constituição Federal Brasileira
CFP	Controle de Fluxo Poligonal
CFTV	Circuito Fechado de Televisão
CICCR	Centro Integrado de Comando e Controle Regional
CICOM	Centro Integrado de Telecomunicações
CIGE	Centro Integrado de Gestão de Emergência
CLS	Classificação de Pessoa ou Veículo
CLV	Cruzamento de Linha Vertical
CME	Coordenadoria de Missões Especiais
CNH	Carteira Nacional de Habilitação
CNJ	Conselho Nacional de Justiça
COE	Centro Integrado de Comunicações
COI	Centro de Operações e Inteligência Dois de Julho
CONDEGE	Colégio Nacional de Defensores Públicos Gerais
CONIPUB	Congresso Internacional de Políticas Públicas
COP	Contagem de Objeto/Pessoa
Covid-19	Corona Virus Disease
CPF	Cadastro de Pessoa Física
DAM	Detecção de Ausência de Movimento
DAP	Detecção de Aglomeração de Pessoas
DOE	Diário Oficial do Estado

DPT	Departamento de Polícia Técnica
DUDH	Declaração Universal de Direitos Humanos
EBIA	Estratégia Brasileira de Inteligência Artificial
EC	Emenda Constitucional
EDPB	Comitê Europeu para a Proteção de Dados
EDPS	Autoridade Europeia para a Proteção de Dados
EDRi	*European Digital Rights*
ES	Espírito Santo
EUA	Estados Unidos da América
FBI	*Federal Bureau of Investigation*
FGV	Fundação Getúlio Vargas
FRVTV	*Face Recognation Vendor Test*
GCM	Guarda Civil Metropolitana
HD	*Hard Disk*
HP	*Hewlett-Packard*
IA	Inteligência Artificial
IDEC	Instituto Brasileiro de Defesa do Consumidor
IECISA	El Corte Inglês
IFF	*Internet Freedom Foundation*
INTERPOL	Organização Internacional de Polícia Criminal
IOT	*Internet of Things*
IT4CIO	*Internet Technology Four*
ITS Rio	Instituto de Tecnologia e Sociedade do Rio
LAI	Lei de Acesso à Informação
LAPIN	Laboratório de Políticas Públicas e Internet
LGPD	Lei Geral de Proteção de Dados Pessoais
LPN	Licitação Pública Nacional
LPR	Leitura de Placas de Veículos
MCI	Marco Civil da Internet
MIT	*Massachusetts Institute of Technology*
MP	Medida Provisória
NIST	*National Institute Stardards and Tecnologys*
ODR	Objetos Deixados/Retirados
PAD	Permanência em Área Designada
PGE-BA	Procuradoria Geral do Estado da Bahia

PI	Ponto de Imagem
PLN	Processamento de Linguagem Natural
PNRH	Plano Nacional para Redução de Homicídios
PNS	Plano Nacional de Segurança Pública
PNSP	Plano Nacional de Segurança Pública de Desenvolvimento Social
PNSPDS	Política Nacional de Segurança Pública e Defesa Social
PPB	*Pilot Partiament Benchmark*
PRODETUR Salvador	Programa Nacional de Desenvolvimento do Turismo em Salvador
PRONASCI	Programa Nacional de Segurança com Cidadania
PTZ	*Pan, Tilt, Zoom*
QR Code	*Quick Response Code*
RF	Reconhecimento Facial
RIPD	Relatórios de Impacto a Proteção de Dados
SAC	Serviços de Atendimento ao Cidadão
SECULT	Secretaria Municipal de Cultura e Turismo
SERPRO	Serviço Federal de Processamento de Dados
SESGE	Secretaria Extraordinária para Grandes Eventos
SINESP	Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas
SSP-BA	Secretaria de Segurança Pública do Estado da Bahia
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
SUSP	Sistema Único de Segurança Pública
TCE-BA	Tribunal de Contas do Estado
TICs	Tecnologias de Informação e Comunicação
TJ-BA	Tribunal de Justiça da Bahia
TRF	Tecnologia de Reconhecimento Facial
TSE	Tribunal Superior Eleitoral
UE	União Europeia
UFBA	Universidade Federal da Bahia
Unifacs	Universidade Salvador
UTP	*Unshield Twisted Par*
VaaS	Vídeo as a Service
Www	*Word Wide Web*

SUMÁRIO

1 INTRODUÇÃO

A sociedade hodierna se destaca pelo avanço da tecnologia e mudanças na forma da inter-relação homem/máquina, principalmente, após a criação da inteligência artificial (IA) e sua aplicação em diversos setores da sociedade, com destaque, neste estudo, para a utilização do reconhecimento facial (RF) automatizado como política de segurança pública.

As revoluções industriais que resultaram na sociedade atual demonstraram a importância do desenvolvimento da tecnologia, especialmente, a partir da Terceira Revolução Industrial, com o desenvolvimento das Tecnologias de Informação e Comunicação (TICs) (CASTELLS, 1999).

As TICs moldaram a nova forma de relacionamento entre economia, Estado e Sociedade e contribuíram para a formação de uma sociedade globalizada (CASTELLS, 2004), mediante a modificação da lógica gerencial produtiva, antes constituída de tarefas repetitivas – Fordismo – para uma cadeia produtiva com incentivo a ampliação de trabalhos intelectuais e das forças microeletrônicas de comunicação, inclusive pelo Estado, na condição de líder ou mediador desse movimento (LOPES, 2008).

A informação começa a ser alçada a um ativo valioso, impulsionada pela criação da IA em 1960, e da internet em 1969, e embalada pela forma de expansão do capitalismo, a partir da década de 1980, cujo destaque se deu com a expansão global da internet comercial, em 1987. Nesse esteio, todos esses acontecimentos contribuíram para a formação da chamada Sociedade da Informação (CASTELLS, 1999) e a criação da Sociedade em Rede (LEVY, 2011).

A partir de 2016 Schwab (2016) cunhou o termo Quarta Revolução Industrial, uma vez que considerou ser um novo paradigma social o avanço da criação de novas tecnologias, como uma fusão em seus domínios físicos, digitais e biológicos que impactam na inter-relação entre o homem e máquina e se aplicam a todos os setores sociais, inclusive para promoção de políticas públicas. São destaques a biotecnologia, IA, robôs, *Internet of Things* (IOT) e a extração e análise de dados – *Big Data*.

A fusão digital homem/máquina, em sua análise sob a ótica do *Big Data,* se perfaz na ideia de utilização dos dados pessoais como matéria-prima, para que, através de análises algoritmas, as empresas de tecnologia possam construir perfis personalizados dos gostos e preferências das pessoas para o oferecimento de seus produtos e/ou serviços, tornando-os mais atrativos e acessíveis (PINHEIRO; FERRAZ, 2021).

O corpo humano passa a ter relevância na criação dos perfis acima mencionados, visto que o perfilamento é realizado por algoritmos que fazem análises biométricas, das emoções e

comportamentos. O perfilhamento algoritmo das pessoas, inclusive são aplicados às relações de trabalho e a cultura da digitalização dos serviços, a exemplo da escolha automatizada de candidatos a vagas de emprego, via IA, aplicações de saúde e telemedicina e aplicativos de prevenção de fraudes via RF.

O poder público também se utiliza da tecnologia de captação dos dados pessoais, via *Big Data*, para a promoção de políticas públicas, com o escopo de perfilar produtos e serviços oferecidos à população, objetivando conferir mais eficiência nos recursos públicos e amplitude da política.

Nesse esteio se destacam a promoção de aplicações com bases de dados integradas e interoperáveis, como a plataforma Gov.br (BRASIL, 2022) para acesso a diversos serviços públicos no Brasil, desenvolvimento de aplicativos para identificação de pessoas que gozariam do direito a benefícios sociais, a exemplo do Auxílio Emergencial e Auxílio Brasil, e ainda, para ações no campo da segurança pública, destaque para o reconhecimento de pessoas foragidas da justiça ou com mandados de prisão em aberto, através de RF, via IA.

Mister ressalvar, entretanto, que um outro efeito secundário e importante é que a captação massiva dos dados pessoais biométricos pode ensejar a realização de grandes bases de dados pessoais para fins que vão além do consumo e personalização de serviços públicos, mas para o exercício do controle e vigilância pelo Estado e pelas empresas que detêm o conhecimento da tecnologia (WERTHEIN, 2000).

Com o desenvolvimento da tecnologia, a vigilância que antes era realizada em espaços fechados e físicos passa a ser realizada também de forma virtual, em um clique, um *cookie*, câmeras de videomonitoramento em locais públicos, muitas vezes, sendo realizada de forma indiscriminada (OLIVEIRA, 2021).

Essa vigilância ostensiva digital é denominada de panóptico digital (HAN, 2018), conceito de vigilância baseado no panóptico de Benthan e que causa preocupações quando há controle excessivo e manipulação de massas quando da implementação de políticas públicas, sobretudo, as de segurança.

A promoção de políticas públicas de segurança envolvendo as TICs se difundiu no Brasil a partir dos anos 2000, mediante estímulo à inovação tecnológica previsto no Plano Nacional de Segurança Pública (PNS) e a necessidade do Estado brasileiro de desenvolver novas ações preventivas e de combate à criminalidade (BRASIL, 2000). Para Alcadipani (2020), a utilização da tecnologia nas ações pelo Estado decorre da tentativa de desenvolver mais ações de inteligência, com menos letalidade e da necessidade do Estado controlar o exponencial crescimento da violência no Brasil.

Em 2013, por exemplo, o Brasil chegou a concentrar 11% dos homicídios de todo o planeta conforme dados extraídos do PNS 2018-2028 (BRASIL, 2018f), o que se mostrou um grande desafio para o Estado propor novas políticas de segurança pública que se mostrassem eficazes e que também tivessem observância às determinações da Constituição Federal Brasileira (CF) de 1988, na qual está determinada a descentralização da segurança pública e a adoção da defesa dos direitos humanos e fundamentais.

Nessa perspectiva, como forma de combate à criminalidade, foram adotadas diversas políticas públicas envolvendo a tecnologia ao longo dos anos no Brasil, com destaque para a área de segurança, do estímulo à utilização da IA, instituído pela Política Nacional de Segurança Pública, no ano de 2018, que trouxe, especificamente, a possibilidade de utilização do RF automatizado para fins de fiscalização de fronteiras, portos, aeroportos e rodovias (BRASIL, 2018f).

O RF via IA pode ser conceituado como a "habilidade que softwares de computador possuem de reconhecer e identificar rostos humanos específicos, a partir de fotos ou vídeos" (COSTA; OLIVEIRA, 2019, p. 6), utilizando-se de conexões de internet e análise de base de dados, a fim de catalogar e detalhar cada indivíduo, processando as "imagens obtidas em um computador, smartphone ou câmera de vigilância" (COSTA; OLIVEIRA, 2019, p. 6).

O uso do RF automatizado para fins de segurança pública já vinha sendo implementado como política pública desde 2001, em diversos países do mundo, sob a espeque de prevenção a ameaças terroristas, em razão dos ataques terroristas de 11 de setembro, nos Estados Unidos da América (EUA) e como forma de combater à criminalidade e violência (OLIVEIRA, 2021).

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

Em 2018, quando foi implementado o RF, os números da segurança pública na Bahia eram alarmantes. Para efeitos comparativos, nesse mesmo ano, a Europa teve 3.993 homicídios (EUROSTAT, 2018) e somente no Estado da Bahia foram computadas 5.620 mortes violentas, entre homicídios, latrocínios e lesões corporais seguidas de morte (G1, 2019b), quase o dobro

[1] O Estado da Bahia já aplicava desde 2008 o videomonitoramento por circuito fechado de televisão (CFTV) como política pública de segurança e foi através da Licitação e do Contrato nº 002/2014/DG/SSP-RDC1, cujo objeto foi a aquisição de câmeras de segurança que, em seu aditivo 1, o licenciamento de softwares de RF, via IA da empresa Huawei foram incluídos como mais uma medida de investimentos na segurança pública.

de mortes de toda a Europa, o que ratificava a necessidade urgente de medidas e investimentos em segurança pública.

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, principalmente nas cidades de Salvador e Feira de Santana, a exemplo do metrô, estação rodoviária e nas ruas que compõem o circuito do carnaval (BAHIA, 2019d), com o objetivo de prevenir e reprimir a criminalidade.

O RF por IA como política pública tem sido apresentada pelo Estado da Bahia como um *case* de sucesso e já foram investidos mais R$ 655 milhões na adoção dessa política, para um prazo de cinco anos (BAHIA, 2021h).

Em 2019, um ano depois de implementada, houve redução de 521 mortes violentas no Estado da Bahia se comparadas a 2018 (G1, 2019b) e, em pouco mais de três anos de funcionamento, já contou com a prisão de mais de 200 pessoas foragidas da justiça, com apresentação de dados oficiais quanto à redução da criminalidade, principalmente nos crimes contra o patrimônio (BAHIA, 2021). Ademais, as imagens captadas também podem ser realizadas para composição de provas judiciais, além de ser uma política pública que reduz custos de pessoal (BAHIA, 2019b) e apresenta menos letalidade.

O RF automatizado está em franco processo de expansão na Bahia, com a proposta de instalação de câmaras de segurança em mais 77 cidades do interior do Estado até 2022, via projeto Vídeo-Polícia Expansão (BAHIA, 2021).

Em 2020 foi lançado o Programa Nacional de Desenvolvimento do Turismo em Salvador (PRODETUR Salvador), no âmbito da Secretaria Municipal de Cultura e Turismo (SECULT), cujo objeto foi a aquisição de equipamentos para melhoria da segurança turística, dentre os quais equipamentos de videomonitoramento que se utilizam de RF via IA para instalação em locais turísticos da cidade de Salvador (ALVES, 2021). Ressalta-se, entretanto, que ainda que seja um projeto do município de Salvador, no que tange ao RF, este será operado pela SSP-BA, por isso sua constância no presente trabalho.

Apesar da apresentação de resultados eficientes quanto à operacionalização da política pública de RF no Estado da Bahia, uma declaração do então governador da Bahia Rui Costa, quando do lançamento da política da tecnologia de RF pela SSP-BA, em 2018, chamou a atenção no que tange ao olhar da compatibilização desta com os direitos da privacidade e proteção de dados pessoais, ao afirmar que a meta do projeto seria o cadastramento de 15 milhões de baianos pelo sistema de RF (BAHIA, 2018).

Naquele momento era publicada no Brasil a Lei nº 13.709/2019, Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018) e o assunto relativo à privacidade e proteção de dados pessoais estava em amplo debate tanto na academia quanto na imprensa brasileira. Por lecionar a matéria de Direito Digital e estudar sobre os assuntos relacionados à aplicação do direito às novas tecnologias, vislumbrou-se alguns questionamentos de como seria a aplicação do RF após a legislação de proteção de dados pessoais.

Ademais, em uma matéria realizada pelo jornalista Murilo Salviano, em 2019, para o programa Fantástico da Rede Globo de Televisão em que se apresentava a política de RF no estado da Bahia, a reportagem deixou a entender que poderia ocorrer a utilização indiscriminada da política pública, mediante o RF realizado a qualquer pessoa que estivesse na Bahia e passasse pelo sistema de videomonitoramento, inclusive quem não estivesse como foragido, desaparecido ou com mandado de prisão em aberto, o que consolidou o interesse em compreender até que ponto essa política pública poderia violar também a liberdade das pessoas.

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

Dessa maneira, diante da possibilidade de possíveis falhas na aplicação da referida política pública que pode levar inocentes a serem presos indevidamente, é importante trazer à baila a possibilidade da utilização da referida tecnologia provocar consequências de possíveis violações aos direitos da liberdade, privacidade e proteção de dados pessoais (NEGRI; OLIVEIRA; COSTA, 2020; SOLOVE, 2011; WERTHEIN, 2000; RODOTÁ, 2008), dentre outros fatores, pelo exercício exacerbado da vigilância e monitoramento das pessoas.

O controle do Estado e das grandes empresas que detém a tecnologia, sem discutir questões éticas e de transparência, sem a oposição das pessoas, se assemelharia a um panóptico digital, favorecendo estados totalitários (HAN, 2018). Nesse esteio, salienta-se, conforme destacado por Norris e Armstrong (1999, p. 113), que "os riscos da sociedade de vigilância ligam-se tradicionalmente ao uso político de informações para controlar os cidadãos" e, quando afirma Rodotá (2008), que as tecnologias de comunicação e informação entram em conflito

com o direito à vida privada das pessoas em razão do direito à autodeterminação informativa, aproximando-se da ideia do panóptico digital.

Assim, em razão da sensibilidade e relevância do tema, pelo alcance dos efeitos sociais da multicitada política pública, coube questionar: *quais os benefícios e desafios da utilização da tecnologia de 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?*

Parte-se do pressuposto de que há necessidade de mais acuidade na aplicação do RF via IA para utilização como política pública de segurança, a fim de evitar possíveis violações de direitos fundamentais das pessoas.

Dessa maneira, o objetivo geral da pesquisa é analisar os principais benefícios e riscos da implementação da política pública de RF, via IA, aplicada pela SSP-BA, visando apresentar e discutir os projetos Vídeo Policiamento – Mais Inteligência na Segurança, Vídeo-Polícia Expansão e PRODETUR Salvador.

Para alcançar esse objetivo, foram definidos como objetivos específicos:

a) Descrever a evolução da sociedade e o impacto das TICs, de forma a perpassar pela Sociedade da Informação, Quarta Revolução Industrial até o desenvolvimento do Panoptismo Digital;
b) Identificar planos e/ou projetos no Brasil realizados a partir de políticas públicas que aplicaram tecnologias de IA, particularmente as de RF;
c) Analisar a utilização – contribuições e limites – da tecnologia de RF utilizada pelo Estado, sob a ótica dos direitos fundamentais da liberdade, privacidade e proteção dos dados pessoais;
d) Investigar a existência de regulamentação legal específica para o uso da IA de RF na segurança pública no mundo e no Brasil;
e) Analisar os principais benefícios e riscos da implementação da política pública de utilização da tecnologia de IA por RF aplicada pela SSP-BA, visando apresentar, discutir e propor melhorias aos projetos Vídeo Policiamento – Mais Inteligência na Segurança, Vídeo-Polícia Expansão e PRODETUR Salvador.

Realizar o estudo ganha relevância em sua investigação teórica-analítica porque seu eixo central refere-se a investigar, sob o olhar da (in)compatibilização com os direitos fundamentais

da liberdade, privacidade e proteção de dados pessoais, a implementação de uma política de segurança pública que envolve uma tecnologia recente, apresentada pelos gestores públicos como solução para diminuição dos índices de criminalidade e violência.

Importante destacar ainda que mais um fundamento para a pesquisa é o fato de que a multirreferenciada política pública também apresenta desfechos diversos em locais que já a implementaram antes do Brasil, a exemplo do Reino Unido, em que há projeto de expansão, e, por outro lado, da cidade de São Francisco, Califórnia, EUA, localizada no Vale do Silício, considerado o berço da tecnologia mundial, por ter sido considerada uma tecnologia invasiva e violadora de direitos fundamentais e que foi determinado o seu banimento.

Ademais, a pesquisa também se mostra importante dentro do seu recorte geográfico, na medida em que se perfaz de um estudo de caso realizado em um estado cuja capital Salvador apresenta uma população em que mais de 81,1% das pessoas se autodeclaram pretos ou pardos (IBGE, 2018), justamente o público-alvo da maior incidência de erros do RF em pesquisas já realizadas pelo mundo, que comprovaram limitações técnicas de acurácia e vieses raciais e sexistas na IA de RF (BUOLAMWINI; GEBRU, 2018; NOBLE, 2018; SILVA T., 2020a).

Ressalta-se que se torna importante investigar se (in)existe uma base legal para os gestores públicos da Bahia utilizarem essa tecnologia de RF na segurança pública, visto se tratar de uma política pública considerada como de alto risco aos direitos fundamentais de privacidade e proteção de dados pessoais (FRANCISCO; HUREL; RIELLI, 2020; SOLOVE, 2011).

Justifica-se ainda o presente trabalho, visto que não foram encontradas dissertações de mestrado ou doutorado que versem sobre o mesmo tema e objetivos, mas tão somente artigos publicados em revistas ou periódicos, o que se torna necessário o aprofundamento do estudo da multicitada política pública.

No que tange à metodologia será realizada uma abordagem bibliográfica nos capítulos teóricos e estudo de caso (YIN, 2005), com apresentação de questionário (GIL, 2002) a Ouvidoria Geral do Estado da Bahia, contendo 10 questões por escrito, de forma aberta, com roteiro de perguntas previamente estabelecidas, que versaram sobre a aplicação da tecnologia de RF como política de segurança pública do Estado da Bahia e foi apresentado mediante preenchimento de requerimento no sítio eletrônico: http://www.ouvidoria.ba.gov.br/, no dia 3 de novembro de 2021.

Destaca-se também que será adotada a técnica de análise documental, de forma complementar, em face dos materiais colhidos pela internet, como leis, diretivas, regulamentos, projetos de lei, editais, palestras na plataforma YouTube, sites de jornais, revistas eletrônicas, portais de notícias e sites de busca – Google acadêmico – e Scielo.

As categorias de análise e principais autores dialogados serão: TICs, IA, RF, políticas públicas de segurança: Castells, Schwab, Han, Foucault, Rodotá, Levy, Vidal, Norris, Armstrong, Buolanwini, Gebru, Alcadipani, Albardeiro, Freitas Filho, Oliveira, S., e Silva, T.; direitos fundamentais e legislação: Bioni, Solove, Cancelier e Doneda.

A pesquisa está organizada em oito capítulos, a contar por esta introdução, na qual apresenta-se o tema, pressuposto, problema de pesquisa, objetivos gerais e específicos, justificativa e síntese metodológica.

O segundo capítulo é dedicado ao estudo da evolução das TICs, sendo abordado o impacto das revoluções industriais com ênfase no desenvolvimento da tecnologia na vida das pessoas e as relações homem-máquina. É exposto a evolução da Sociedade Disciplinar até a Sociedade do Controle, marcada atualmente pela vigilância e desenvolvimento de um controle do Estado e das grandes empresas de tecnologia (HAN, 2018).

O terceiro capítulo dedica-se às tratativas sobre a utilização das TICs como política pública de segurança, através da identificação e apresentação de planos de desenvolvimento de políticas de segurança pública no Brasil, com descrição das principais políticas de segurança já adotadas, se utilizando da tecnologia, mas com destaque para a utilização da IA de RF.

No quarto capítulo são apresentadas as vantagens e as limitações técnicas da tecnologia, com ênfase para a tratativa sobre vieses algoritmo, mas especificamente sobre a existência de racismo e sexismo algoritmo.

O quinto capítulo trata sobre a utilização da política de RF com base nos direitos fundamentais da liberdade, privacidade e proteção de dados pessoais, trazendo conceitos, histórico e aspectos regulatórios que envolvem os referidos direitos.

No sexto capítulo é apresentada uma discussão quanto à existência ou inexistência de regulação específica sobre o RF utilizado na segurança pública no mundo, trazendo alguns casos como Reino Unido, EUA e Europa, bem como o Brasil. Nesse esteio, são dispostas algumas possíveis formas de regulamentação legal, através de princípios ou ainda de projetos de lei. São também apresentadas discussões levantadas por entidades de direitos humanos que defendem o banimento da referida tecnologia na segurança pública.

Em seguida, devido à escolha metodológica da dissertação, no sétimo capítulo serão descritas as opções metodológicas utilizadas para a concretização da pesquisa, indicando o método utilizado, contribuições e desafios, autores pesquisados, categorias de análise para cada objetivo específico, bem como, a descrição do percurso metodológico utilizado.

O oitavo capítulo é dedicado às análises empíricas, e apresenta a política pública de RF, via IA, aplicada pelo Estado da Bahia através do programa Vídeo Policiamento – Mais

Inteligência na Segurança e Vídeo-Polícia Extensão e ainda o PRODETUR Salvador, projeto de segurança turística promovido pelo munícipio de Salvador, mas que contém, em seu escopo, o RF, via IA, com interoperabilidade com a SSP-BA. Neste capítulo são realizadas análises, discussão dos resultados e proposições de melhoria para aplicação da multirreferida política pública.

Ao fim e ao cabo, são apresentadas as conclusões da pesquisa, apresentando os resultados apresentados sobre as análises dos principais benefícios e riscos da implementação da política pública de RF, via IA, aplicada pela SSP-BA, assim como as limitações da pesquisa, em especial pela calamidade pública provocada pela pandemia de Corona Virus Disease (Covid-19) e seus impactos na sociedade e as perspectivas de estudos.

2 REVOLUÇÃO INDUSTRIAL E O SURGIMENTO DAS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO

Alguns autores analisam a evolução da sociedade pela perspectiva de ondas, as quais impulsionaram as transformações sociais, econômicas, políticas e culturais em cada sociedade. Essas mudanças foram particularmente impulsionadas pelas revoluções industriais. Segundo Peck (2019), a primeira onda foi a Era Agrícola na qual a propriedade era sinônimo de poder e riqueza.

A segunda onda foi iniciada com a Primeira Revolução Industrial, no século XVIII, e foi marcada pelo surgimento da máquina a vapor e da transição da manufatura para a produção em grande escala (SCHWAB, 2016). Com essa revolução, a noção de riqueza passa a ser a junção de propriedade, trabalho e capital (PECK, 2019).

A terceira onda, chamada de Era da Informação, foi iniciada a partir da Segunda Revolução Industrial e algumas das suas características permanecem até os dias atuais. A Segunda Revolução Industrial teve início na segunda metade do século XIX, sendo marcada por importantes transformações sociais, estimuladas através da invenção da energia elétrica, da utilização do petróleo em substituição ao carvão, bem como da fabricação dos motores de explosão e do desenvolvimento dos meios de comunicação, como o telefone e telégrafo (MENEZES, 2022). No contexto dessas mudanças, a invenção dos meios de comunicação apresentou-se como condição fundamental para as transformações que viriam a seguir, sendo caracterizada como a "produção em grande escala, de massificação, centralização de poder e estandardização ditado pela Era Industrial" (PECK, 2019, p. 52). Nesse esteio, surge a tecnologia digital.

Já a Terceira Revolução Industrial foi iniciada com o fim da Segunda Guerra Mundial e é caracterizada pela revolução digital e pelas TICs (MENEZES, 2022). A informação, segundo o artigo 4º, inciso I, da Lei de Acesso à Informação LAI, Lei nº 12.257/2011 (BRASIL, 2011b), são dados "processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato". A informação aliada à tecnologia passa a ser um ativo importante para a sociedade.

As TICs, segundo Castells (1999, p. 67), podem ser definidas como o "uso de conhecimentos científicos para especificar as vias de se fazerem as coisas de uma maneira reproduzível". Destacam-se o desenvolvimento de software, hardware, telecomunicações, radiodifusão, optoeletrônica e engenharia genética.

Para Rodrigues (2016, p. 15), as TICs “podem ser definidas como o conjunto total de tecnologias que permitem a produção, o acesso e a propagação de informações, assim como tecnologias que permitem a comunicação entre pessoas”. Nesse sentido, a partir de 1950 o desenvolvimento tecnológico teve um papel fundamental na mudança econômico e social da época, haja vista que possibilitou o aumento da produção além da demanda e a consequente expansão do mercado.

A revolução tecnológica concentrada nas TICs modificou a base da sociedade, de forma a proporcionar uma interdependência global, através de nova forma de relacionamento entre economia, o Estado e a sociedade (CASTELLS, 2004), passando dos “insumos baratos de energia como na revolução industrial” (WERTHEIN, 2000, p. 1) para os “insumos baratos de informação propiciados pelo avanço na microeletrônica e telecomunicações” (WERTHEIN, 2000, p. 1).

Em 1969, na Terceira Revolução Industrial, foi criada a internet para fins militares na Guerra Fria que, inicialmente, foi denominada de *Advanced Research Projects Agency Network* (ARPANET). A internet foi expandida para utilização comercial quando da criação, por Tim Berners-Lee, em 1987, da *Word Wide Web*, conhecida por www, que é um sistema de documentos armazenados na internet que permite aos usuários acessarem textos em formato digital (AUGUSTO, 2019).

A internet, quando do surgimento, foi considerada uma tecnologia restrita, limitada. Em 1993, a *Word Wide Web* foi lançada em domínio público, gratuita e com liberação de suas ferramentas, a abertura do software-base permitiu a expansão e democratização da utilização da internet (AUGUSTO, 2019), mediante a ampliação da comunicação entre as pessoas com a consequente expansão global das informações, de forma que as telecomunicações e a informática se tornaram mais acessíveis a todos (LEVY, 1999).

A rápida expansão da internet fez com que ela se tornasse “o meio indispensável e a força propulsora na formação da nova economia, erigidas em torno de normas e processos novos de produção, administração e cálculo econômico” (CASTELLS, 2004, p. 72).

Para que a internet pudesse alcançar sua rápida expansão há uma imensa engenharia envolvida através da instalação de malha de meios de comunicação, desde micro-ondas, fibra ótica, fios de telefone, cabos submarinos transoceânicos, transmissões por satélites, tudo isso através do controle de computadores para o processamento dessas informações. (TAKAHASHI, 2000).

Com a disseminação global da internet e da informação surge a denominada **Sociedade da Informação ou Sociedade Informacional**, nomenclatura criada por Castells (1999), que

representou a forma como o sistema capitalista de produção passou a se reestruturar a partir da década de 1980.

O avanço tecnológico como um novo paradigma resultou em grande parte de ação do Estado como líder ou mediador, que permitiu revelar uma restruturação do capitalismo muito motivado pelo avanço das tecnologias e sua interação com os sindicatos locais, o que gerou um processo de transformação social (GUEVADA, 2000 *apud* WERTHEIN, 2000), "que teria no trabalho criativo e cultura da inovação fontes de produtividade e valorização econômica" (LOPES, 2008, p. 4) mais humanitário porque substitui os trabalhadores do **fordismo** e as tarefas repetitivas pelo trabalhador autônomo e mais instruído (CASTELLS, 1999).

Como características do paradigma tecnológico, a informação passa a ter uma importância singular, haja vista que passa a ser a matéria-prima da atuação do ser humano na informação propriamente dita e não apenas como meio de ser dominado para ampliar o uso da tecnologia (CASTELLS, 1999; WERTHEIN, 2000).

Importante mencionar a flexibilidade como outra característica desse paradigma tecnológico da Sociedade da Informação, visto a capacidade de reconfiguração em uma sociedade marcada pela mudança e fluidez organizacional (CASTELLS, 1999; WERTHEIN, 2000).

Ainda destacam-se a penetrabilidade, uma vez que como a informação é parte da atividade humana, os processos da existência individual ou coletiva de todos acabam sendo afetados pela nova tecnologia, e lógica das redes: quando as redes se difundem, o crescimento tecnológico é exponencial, dessa forma a difusão da informação em rede amplia a sua importância e implementação em qualquer tipo de processo e crescente convergência das tecnologias, através da interligação das áreas de saber que se utilizam da tecnologia (CASTELLS, 1999; WERTHEIN, 2000).

No que tange a centralidade que as TICs conquistaram na contemporaneidade, com base no desenvolvimento da internet, é importante ressalvar dois posicionamentos: o primeiro, se refere ao impacto social e na esfera produtiva que emerge um novo regime de acumulação (LOPES, 2008); o segundo, a defesa de que as TICs podem ajudar a reparar mazelas sociais pelo seu caráter democratizante (CASTELLS, 1999).

Lopes (2008) se posiciona no sentido de que o fundamento do caráter eminentemente democrático e socializante das TICs, que diminuiria assimetrias no sistema, defendido por Castells (2004), decorre de uma leitura distorcida das macromudanças econômico-sociais e justifica posicionamento no sentido de que estar diante de uma rede com conectividade mundial,

com convergência em diversas mídias e com produtos intangíveis, como a informação, seria uma espécie de capitalismo da informação.

As TICs modificam os modos de produção mudando "profundamente a lógica reprodutiva e o sistema gerencial a partir da ampliação das forças produtivas microeletrônicas, da comunicação e do trabalho intelectual" (LOPES, 2008, p. 1). Há a intelectualização de forma geral quanto aos processos de trabalho e de consumo, bem como exigências de novas habilidades para se alcançar o sucesso competitivo, mas, segundo Lopes, (2008), seria um equívoco eleger a tecnologia como um paradigma de mudança.

> [...] pois a centralidade econômica das TICs, da informação e do conhecimento nos dias atuais é reconhecer que o capitalismo – movido por suas próprias crises e conflitos entre o capital e o trabalho e não podendo mais valorizar-se, como antes, na esfera da indústria propriamente dita – foi obrigado a espraiar-se para áreas mais **imateriais** como a cultura e os serviços, ou a ver na financeirização uma excelente oportunidade, ainda que episódica, de ganhos fáceis. (LOPES, 2008, p. 1, grifo do autor).

Ainda, para Vidal (2014), a internet e seus espaços mediáticos – ciberespaços – se estabeleceram como "ontológica categoria central da contemporaneidade", digitalizada, interativa e comutável, com matriz na rede global de computadores, e mudaram a interação social com a tecnologia mediante a utilização de artefatos tecnológicos nas interações humanas culturais, impactando na análise quanto a essas novas relações com o poder, sendo uma utopia o aspecto democratizante de que não há hierarquia de poder.

No final da década de 1990, o poder de comunicação da internet provocou uma nova mudança tecnológica, a dos microcomputadores, descentralizados, autônomos por meio de dispositivos de processamento de dados distribuídos ao redor de servidores da web (CASTELLS, 1999, p. 89), o que contribuiu para a organização da sociedade em rede.

Levy (2011) apresenta o termo **rede** como **ciberespaço**, que seria um novo meio de comunicação originada da interconexão mundial de computadores, em que as pessoas navegam na internet, adquirem e compartilham novos conhecimentos. Para Levy (2011, p. 7):

> [...] novas maneiras de pensar e de conviver estão sendo elaboradas no mundo das telecomunicações e da informática. As relações entre os homens, o trabalho, a própria inteligência dependem, na verdade, da metamorfose incessante de dispositivos informacionais de todos os tipos. Escrita, leitura, visão, audição, criação, aprendizagem são capturadas por uma informática cada vez mais avançada.

Com a criação e desenvolvimento do ciberespaço e as novas formas de pensar e conviver desenvolvidas pela interação entre os homens e a informática se perfez no desenvolvimento de uma **cibercultura**, que seria o conjunto de técnicas materiais e intelectuais de práticas, modos de pensamento e de valores que surgem ou evoluem em razão da relação das pessoas com o **ciberpespaço** (LEVY, 2011, p. 17).

A interação cada vez mais imponente entre os homens e a informática, deu origem ao surgimento de novas tecnologias que provocaram não somente impactos relacionados à cultura ou a objetivos sociais e econômicos, mas até mesmo impactos biológicos na humanidade. Para Schwab (2016), essa nova forma de interação e desenvolvimento tecnológico significou que a humanidade adentrou na Quarta Revolução Industrial[2].

2.1 QUARTA REVOLUÇÃO INDUSTRIAL: AVANÇOS TECNOLÓGICOS, *BIG DATA* E INTERAÇÃO HOMEM-MÁQUINA

A Quarta Revolução Industrial trouxe transformações em toda a sociedade e alterou a maneira como as pessoas vivem, trabalham e se relacionam. Há uma mudança de paradigma em curso no modo de se relacionar das pessoas com o trabalho, diversão e existência social, marcada pela "fusão dessas tecnologias e a interação entre os domínios físicos, digitais e biológicos" (SCHWAB, 2016, p. 17).

Schwab (2016) justifica a Quarta Revolução Industrial mediante as novas tecnologias e apresenta três razões: 1) velocidade da difusão da tecnologia; 2) profundidade e 3) impacto no sistema entre países – interno e externamente, atingindo socialmente a economia, política e forma de novos negócios.

Nesse esteio, destacam-se os avanços tecnológicos de desenvolvimento da biotecnologia, IA, robótica, IOT, veículos autônomos, impressões em terceira dimensão (3D), computação quântica, bitcoins, economia compartilhada, blockchain, sistemas em nuvens, dentre outros que redefinem o ser humano ampliando sua longevidade, saúde e cognição (SCHWAB, 2016; ZUBOFF, 2018).

Para Schwab (2016) é importante aplicar quatro tipos de inteligência na criação dessas tecnologias, quais sejam: contextual, emocional, inspirada e física, que seriam estruturadas pelo aumento da conscientização dos diversos setores sociais, mediante o desenvolvimento de proposições éticas e a restruturação dos sistemas políticos, econômicos e sociais. Para Schwab

[2] Termo cunhado por Klaus Schwab, em 2016, no Fórum Econômico de Davos (Suiça).

(2016), a sociedade deve assumir a responsabilidade coletiva por um futuro em que a inovação e tecnologia sejam sustentáveis e sirvam ao interesse público.

Se por um lado há incerteza no desenvolvimento tecnológico nos desdobramentos gerados pela Quarta Revolução Industrial, uma vez que a Sociedade da Informação ainda tem que lidar com muitos desafios de caráter técnico, econômico e até mesmo legal, a exemplo da automação dos processos e produtos e o consequente desemprego provocado pela falta de qualificação para operacionalização das novas tecnologias e ainda a invasão de privacidade do indivíduo, por outro lado a própria evolução do paradigma já faz com os desafios acima sejam reduzidos, por exemplo, uma restruturação do emprego e qualificação dos trabalhadores e o desenvolvimento social (LEAL, 1996 *apud* WERTHEIN, 2000).

Hodiernamente a contribuição das TICs para a melhoria de alguns campos na sociedade é explícito, principalmente pela necessidade de rápida adaptação pela qual a humanidade foi obrigada a assumir em razão da pandemia de Covid-19, iniciada em 2020 e que permanece até os dias atuais.

O isolamento social necessário à contenção do avanço da pandemia foi um verdadeiro estopim para a digitalização de serviços e produtos. No âmbito da saúde se destacam, dentre outros, a regulação das consultas por teleconferências, os aplicativos com orientações de saúde; no campo da educação, o desenvolvimento de aulas on-line e no campo econômico o desenvolvimento de aplicativos para cadastramento de usuários beneficiários de políticas públicas, visando ampliar o acesso das pessoas aos seus direitos.

Um aspecto importante para o desenvolvimento dessas novas tecnologias é justamente a extração e análise de dados, processos importantes para compreender o *Big Data*. Os dados passam a ser a matéria-prima, fonte de riqueza de um capitalismo, definido por Zuboff (2018) como **capitalismo da vigilância**, que seria uma "nova forma de capitalismo da informação que procura prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado" (ZUBOFFF, 2018, p. 18).

Para Zuboff (2018) são fontes de dados: dados derivados de transações econômicas mediadas por computadores; dados mediados por computador de modo exponencial, que se utilizam de uma estrutura integrativa entre corpos e lugares conectados à internet, como a IOT, drones, carros automatizadas, IA, bancos de dados governamentais e corporativos, "câmeras de vigilância públicas e privadas, smartphones, satélites, curtidas do Facebook" (SAMPAIO et al, 2021, p. 5), buscas no Google, e-mails, localizações e compras (SAMPAIO et al, 2021, p. 5).

O Quadro 1 demostra de forma resumida quais as áreas, fontes de dados e as técnicas que são utilizadas para o tratamento de dados, de forma a extrair perfilamento e valor comercial aos dados.

Quadro 1 – Técnicas de *Big Data Analysis*

Área	**Fontes de dados**	**Técnicas**
Análise/mineração de textos, *Information extraction.*	Redes sociais, e-mails, blogs, fóruns on-line, questionários, relatórios, notícias, registros de *call centers.*	*Text summarization, question answering, sentiment analysis.*
Análise de áudio.	Dados de *call centers*, área da saúde.	*Automatic-speech recognition, phonetic-indexing, search.*
Análise de conteúdo de vídeo.	Vídeos de segurança – circuitos internos; geração descentralizada de vídeos – YouTube.	*Server-based/edge-based architecture.*
Análise de redes sociais.	Redes sociais, blogs, microblogs, social, compartilhamento de mídias, sites de respostas/perguntas, wikis.	*Content-based analytics, structure-based analytics – community detection, social influence analysis, link prediction.*

Fonte: Silva Neto, Bonacelli e Pacheco (2020).

Ressalva-se que o rápido desenvolvimento dessas tecnologias, principalmente mais preditivas, provocadas pela acumulação, extração e análise de dados – *Big Data*, uma vez integrada e interconectadas com as pessoas, como a IA e a IOT causam imensas inquietações sob os efeitos destas no futuro da humanidade pelo seu potencial de modificação das relações homem/natureza para homem/máquina. Os dados de análises comerciais são extraídos dos seres humanos através da análise de sua biometria, do estudo do seu corpo, seu comportamento e emoções.

O corpo humano interconectado à tecnologia começa a ser um fator de preocupação quanto aos possíveis efeitos dessa relação (ZUBOFF, 2018; SIQUEIRA; LARA, 2020; WERTHEIN, 2000), sob a ótica da vigilância ostensiva e do controle, principalmente no que tange a utilização deste como forma de expansão de um **capitalismo da vigilância** (ZUBOFF, 2018), em que o poder é concentrado e exercido pelo Estado e empresas de tecnologia sem que muitas vezes as pessoas percebam que estão sendo controladas.

Para Werthein (2000), os avanços tecnológicos e as melhorias no desenvolvimento social provocados pela aplicação da tecnologia na vida das pessoas superam os possíveis desafios dessa aplicação e interconexão entre tecnologia e ser humano, contudo, é feito uma ressalva de que o sentimento de perda de controle das pessoas sobre sua vida e a perda de identidade é um desafio preocupante e carecem de estratégias eficientes de intervenção para sua minimização.

A relação de utilização do corpo humano passa a ter primordial relação com o avanço das novas tecnologias de informação e controle social, contudo, a importância do corpo humano como forma de controle e poder não é algo novo, por isso para se entender o atual fenômeno de integração digital, se faz necessário dispor sobre a ideia do panóptico de Bentham e a origem da sociedade da disciplina de Foucault (1999) que evoluiu e chegou até os dias atuais de integração tecnologia/humano para a formação da sociedade da vigilância e controle digital panoptismo digital (HAN, 2018).

2.1.1 O corpo humano como forma de exercício da vigilância e controle: da Sociedade Disciplinar à Sociedade do Controle Digital

A sociedade perpassou por uma evolução quanto a forma de controle do Estado na vida das pessoas, mediante a qual se traz à baila, inicialmente as questões relativas ao sistema penal. Atualmente com a influência da tecnologia, o Estado conseguiu ampliar o seu poder, agora se utilizando da vigilância e do controle em outros setores da vida, tais como economia, educação, com destaque para a segurança pública.

O sistema penal, em seus primórdios, contava com o imperativo da **vingança privada**, mediante o qual cada pessoa estava autorizada pelo Estado para reprimir violações do direito da forma que lhe conviesse, com estudos remotos ao século XIII. Após, surge a fase da **vingança divina**, em que o sacerdote é que se torna o responsável pela aplicação das penas e definições sobre o futuro dos infratores, posteriormente o sacerdote perde poder dentro da sociedade e este poder punitivo é transferido para o monarca, nasce assim o poder punitivo estatal, também chamado de **vingança pública** (VIDAL, 2014, p. 19-20).

No final do século XVIII, o corpo humano passa a ser considerado como uma máquina que se pode controlar, nascendo uma mecânica do poder "através da qual se pode ter o domínio dos indivíduos para que façam o que quer o Estado e, sobretudo, operem com as técnicas, rapidez e eficácia exigidas" (VIDAL, 2014, p. 23), contexto este aplicado principalmente quanto ao tratamento dado aos prisioneiros.

Em 1794, Jeremy Bentham concebeu a ideia de projetar um prédio prisional, com uma arquitetura que permitisse o máximo controle das pessoas (OLIVEIRA, 2021) nos planos físicos e estrutural, controle este exercido pela vigilância, o Panóptico. Vigiar consiste em "assistir, ouvir ou registrar as atividades de um indivíduo" (SOLOVE, 2008, p. 154), "monitorar, ouvir, interceptar" (VIDAL, 2014, p. 40).

Ao analisar o Panóptico de Bentham, Foucault (1999) vai além do pensamento do controle por vigilância e começa a aplicar uma técnica de controle dos corpos, através da análise da utilidade e docilidade destes, comumente chamada de disciplina. Nesse diapasão, outras instituições da sociedade, como escolas, igrejas, hospitais, quarteis, etc. também começam a se valer da sujeição de aptidões e forças como forma de controle através da disciplina (FOUCAULT, 1999; VIDAL, 2014).

Segundo Vidal (2014), para Foucault, o controle na sociedade disciplinar se daria mediante o quadriculamento dos indivíduos, separação dos corpos em celas, com lugares determinados para otimizar a vigilância e controle estatal, assim já se percebe a ideia do controle estatal absoluto e não apenas dos indivíduos que cometeram crimes.

A arquitetura estrutural do panóptico privilegia o fato de que haja poucos observadores para supervisionar muitas pessoas. O objetivo do panóptico, segundo Foucault (1999, p. 240), é "fazer com que a vigilância seja permanente em seus efeitos, mesmo se é descontinua em suas ações, que a perfeição do poder tenda a tornar inútil a atualidade de seu exercício". A ideia de vigilância incessante proporciona um aspecto subjetivo do efeito da disciplina, uma sujeição fictícia.

Assim, as pessoas se autodisciplinam com a ideia do olhar onipresente, com a invisibilidade do poder disciplinar, que tem um efeito de "se apropriar e retirar, tem como função maior adestrar para retirar e se apropriar ainda mais e melhor" (FOUCAULT, 2001, p. 43).

A vigilância é a principal engrenagem do poder disciplinar. Ela contribui para individualizar os sujeitos a ela submetidos e generaliza a disciplina. Para Foucault (2001, p. 239), a vigilância assegura uma "distribuição infinitesimal do poder".

Segundo Schneider e Miranda (2020, p. 3), o pensamento de Foucault concretizou a análise da transição da estrutura física do panoptismo para uma tecnologia de poder "utilizada com a finalidade de obter o máximo de proveito e domínio sobre os indivíduos (homem-corpo), sempre conectada a um capitalismo liberal em ascensão, de modo a torná-lo o mais eficaz possível".

A vigilância ostensiva se baseia na disciplina e mobiliza as forças sociais, levando ao aumento da produção e da economia, fabricando indivíduos úteis, mais dóceis e menos custosos econômica ou politicamente (FOUCAULT, 1999; POGREBINSCHI, 2004), pelo que pode ser constatado a Sociedade Disciplinar.

> O momento histórico das disciplinas é o momento em que nasce uma arte do corpo humano, que visa não unicamente o aumento das suas habilidades, nem tampouco aprofundar sua sujeição, mas a formação de uma relação que no mesmo mecanismo o torna tanto mais obediente quanto é mais útil, e inversamente. Forma-se então, uma política das coerções que são um trabalho sobre o corpo, uma manipulação calculada dos seus elementos, de seus gestos, de seus comportamentos. (FOUCAULT, 1999, p. 119).

Foucault (2011) analisa o corpo humano de forma que possa ser manipulado em seus comportamentos como um mecanismo de poder para se alcançar a disciplina, quanto mais informações sobre as pessoas, maior o poder de controle.

Nesse esteio surge a biopolítica, de forma que o poder passa a ser exercido sobre populações, através do foco em corpos coletivos, sob o espeque de preservação da vida através da extinção de possíveis ameaças ao bem-estar social com base em ideais econômicos liberais (SCHNEIDER; MIRANDA, 2020).

Com o avanço tecnológico, o Estado e a iniciativa privada começam a se utilizar das TICs como forma de controle e vigilância, a exemplo do desenvolvimento de *softwares* e outras tecnologias mais potentes, como a IA, para promoção de políticas públicas, inclusive de segurança, sob o argumento de políticas públicas mais modernas, eficientes e menos letais que fazem parte da sociedade digital (OLIVEIRA, 2021).

Uma vigilância que se aplica a contextos, lugares, períodos de tempo, de forma geral e não específica a uma pessoa, mas a categorias de pessoas, uma vigilância generalizada (NORRIS; ARMSTRONG, 1999).

A vigilância é exercida a cada *click* na web, seja em um site ou em uma rede social, através de um *cookie*, que são "pequenos arquivos de texto que contêm várias informações sobre os visitantes de um website. A principal função do cookie é identificar e armazenar informações desses usuários" (DONDA, 2020, p. 50), ou de um pixel, ou ainda em situações corriqueiras da vida, principalmente nos centros urbanos, como a vigilância realizada pelas câmeras de vídeo em locais públicos que estão sendo usadas de maneira generalizada tanto pela iniciativa privada quanto pela administração pública. Assim, Han (2018) apresenta essa nova forma de vigilância e controle como uma nova forma de panóptico, a qual denomina **panóptico digital**.

Koerner (2020, p. 4) apresenta a sociedade atual como um momento "pós-disciplinar, da vigilância automatizada que opera ambientalmente e não supõe a internalização do olhar pelo sujeito. O simbólico é deslocado pelo atual, torna-se real o olhar onisciente que não necessita um vigiado consciente".

O centro do poder do panóptico digital não se encontra totalmente atrelado ao Estado, ou ao poder familiar, ou de instituições, esse poder passa a ser também das grandes corporações que controlam as tecnologias, mediante a coleta, armazenamento e processamento de dados pessoais (OLIVEIRA, 2021, p. 93), inclusive fornecidos pelas próprias pessoas, através de autoexposição (HAN, 2018), gerando assim um controle geral e multilateral (VIDAL, 2014).

A diferença entre o panóptico de Benthan e o panoptico digital está que, no primeiro, o isolamento social é condição de aplicação da vigilância ostensiva, ao passo que, no panóptico digital, a vigilância pressupõe a conexão e comunicação intensa de seus habitantes (HAN, 2018). No lugar do *Big Brother*[3], entra o *Big Data* (HAN, 2018, p. 122).

Segundo Zuboff (2018), o Estado e as grandes corporações detentoras das tecnologias de reconhecimento de pessoas, ao se tornarem onipresentes e vigilantes, representam um risco para a sociedade, no que tange a possibilidade da utilização abusiva das informações biométricas das pessoas, seus gostos, seus passos, sua liberdade em detrimento de fins econômicos ou políticos escusos, que é uma consequência do **capitalismo da vigilância**.

Assim, a expansão dessas tecnologias de identificação e comunicação, catalogação e controle de pessoas mediante o compartilhamento intenso de dados, se torna ainda mais arriscada pela potencial nocividade de controle e manipulação das massas, seja pelas limitações relacionadas a possíveis falhas da aplicação da tecnologia, ou ainda a utilização desta por estados totalitários, tecnoautoritarismo, que violariam o direito à privacidade das pessoas.

Segundo Barbosa (2021), o tecnoautoritarismo são ferramentas do Estado baseado em tecnologias que promovem coleta massiva e indiscriminada de dados pessoais e o uso dos dados como ferramenta de controle.

Para Solove (2008), o excesso de vigilância e controle pode ser nocivo à democracia, porque pode afetar negativamente a liberdade, a criatividade e o autodesenvolvimento das pessoas.

Por outro lado, Koerner (2020, p. 4) apresenta o posicionamento de que a vigilância seria algo inerente à lógica de exploração dos dados "pois só se usam metadados, e o objetivo da elaboração de perfis individuais seria a melhoria dos serviços". Koerner (2020, p. 4) também defende a restrição de controle e regulação das TICs e autorregulação pelas empresas de suas tecnologias:

[3] O *Big Brother* é um grande irmão que, dentro das ideias de George Orwell, no livro 1984, atua como um poder dentro de uma sociedade fictícia em que tudo vê e controla todos.

> a vigilância para extração de dados é inerente à sua lógica e não será controlada ou eliminada por restrições legais ou regulações. A tendência não seria um poder instrumentário global, mas batalhas por monetização e controle. As empresas viriam a criar ambientes fechados, com maior respeito à privacidade, mas com identificação constante dos usuários. [...] (KOERNER, 2020, p. 4).

Koerner (2021, p. 4) conclui informando que a privacidade seria um direito subjetivo mercantilizável pelo seu titular, cuja liberdade de escolha se exerceria ao contratar os termos de uso para a extração dos dados realizada pelas empresas. Nesse diapasão, Batkins (2019) afirma que o aspecto da vigilância não seria um desafio ao desenvolvimento das TICs, conforme defende Zuboff (2018), pois seria inerente ao desenvolvimento da tecnologia.

A aplicação das TICs pelo Estado na promoção de políticas públicas, principalmente no âmbito da segurança pública é algo não pacificado, haja vista possíveis conflitos entre a utilização da tecnologia e as dicotomias entre controle e vigilância versus direitos fundamentais das pessoas, por isso, nos próximos capítulos, serão explorados essas questões como medidas (in)eficientes de aplicação na segurança pública.

3 O USO DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO COMO POLÍTICA DE SEGURANÇA PÚBLICA

A evolução da sociedade e aplicação das TICs se perfizeram também como um mecanismo de utilização da tecnologia para prevenção e repressão de crimes, contribuindo para o desenvolvimento de políticas de segurança pública no Brasil menos letais e mais eficientes (ALCADIPANI, 2020).

A segurança pública pode assim ser definida como

> um conjunto integrado e otimizado envolvendo instrumentos de coação, justiça, defesa dos direitos, saúde e social. Portanto, a segurança pública se inicia com prevenção e se finda na reparação do dano, no tratamento das causas e na reinclusão na sociedade do autor do ilícito. (LIMA; OLIVEIRA; COSTA, 2021, p. 106).

Historicamente, na época colonial brasileira, os crimes atentavam contra a vontade do Soberano e eram tratados como faltas morais ou religiosas. As atribuições policiais e judiciais eram exercidas por poucos cargos dentro da hierarquia de poder e as práticas de punição aos infratores eram realizadas mediante degredo, para pessoas mais abastadas, e de açoite, para os escravos. As práticas de investigação eram feitas por suspeitas sobre o indivíduo e as provas colhidas mediante tortura judicial (OBSERVATÓRIO DE SEGURANÇA, 2020).

A segurança pública sob o aspecto estatal remonta a 1808, com a criação da Intendência Geral de Polícia e Corte do Estado do Brasil, na cidade do Rio de Janeiro, que tinha como função delegar e desempenhar funções de polícia judiciária, com o estabelecimento de poderes de fiscalização e aplicação de punições (MARCINEIRO; GIOVANNI, 2005). Em 1824, o Brasil promulgou sua Constituição, um Código Criminal, em 1830, e um Código de Processo Criminal, em 1832. A lei penal começou a entender o crime como infração penal e o sofrimento físico passou a dar lugar a penas como o degredo e a privação de liberdade (OBSERVATÓRIO DE SEGURANÇA, 2020).

Com o advento das Constituições de 1934, 1937 e 1946 e ainda com o Código Penal de 1940 e o Código de Processo Penal de 1941 ocorreram diversas mudanças pelos entes integrantes da segurança pública[4] quanto ao estabelecimento de normas relativas ao processamento de crimes através de uma centralização e racionalização da administração pública, todavia, com a Ditadura Militar, os direitos constitucionais dos investigados e

[4] Ministério Público, Polícias, Magistrados e Júri.

capturados pelas polícias e para os que estavam internados em manicômios foram relegados, mediante a adoção de torturas e degradações, segundo notícias da imprensa à época (OBSERVATÓRIO DE SEGURANÇA, 2020).

A democratização do Brasil iniciou em 1985 e foi consagrada com a CF de 1988, que, em seu artigo 5º, *caput*, então vigente, veio a disciplinar a segurança pública como um direito fundamental, como dever do Estado, direito e responsabilidade de todos a ser exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio (artigo 144).

Ainda, a CF de 1988 descentralizou a segurança pública mediante atribuições e responsabilidades atribuídas às policias 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 nova configuração político-institucional após a CF de 1988, baseada na instituição da defesa dos direitos humanos, os institutos jurídicos tradicionais do Brasil não promoveram a integração dos direitos definidos pela CF com as práticas das polícias e do judiciário nas aplicações punitivas, aliado a isso, houve um exponencial crescimento da violência e criminalidade e cada vez mais a segregação da iniciativa privada, vide as iniciativas de condomínios fechados, gradeamento de casas, adoção de equipamentos de segurança e contratação de segurança privada (OBSERVATÓRIO DE SEGURANÇA, 2020).

Para tentar se proteger da violência crescente, o Estado passou a investir mais em armas e equipamentos, e a iniciativa privada em grades, muros e dispositivos eletrônicos OBSERVATÓRIO DE SEGURANÇA, 2020). O sentimento de insegurança e a cultura do medo inundaram a sociedade, sobretudo nos grandes centros urbanos e diante dessa nova problemática, segundo Barbosa e Santos (2009), não há a possibilidade da resolução da violência somente com ações e políticas repressivas.

Segundo a Política Nacional de Segurança Pública e Defesa Social (PNSPDS) de 2018-2028, o Brasil, em 2013, concentrava 11% dos homicídios do planeta[5], e afirma: “Os dados do Ministério da Saúde indicam que o Brasil passou de 11,7 homicídios por 100 mil habitantes em 1980 para 30,3 em 2016, o que resultou na morte de 1,4 milhões de pessoas em território nacional no período” (BRASIL, 2018f).

[5] “O documento que analisou a taxa de violência letal em 121 países no ano de 2013 registra que o Brasil, com 2,8% da população mundial, concentra 11% dos homicídios do planeta, realidade que, infelizmente, mostra tendência no sentido de agravar-se a cada ano” (BRASIL, 2018, p. 23).

Ademais, o crime organizado está cada vez mais munido de armas de grosso calibre e se valendo de novas tecnologias e estratégias em ações que dificultam as ações de segurança pública e a mentalidade de apenas utilização da força bruta estatal. Assim, o Estado tem que investir em agentes de segurança pública, de forma a ampliar os conhecimentos científicos, se aprimorar e utilizar as tecnologias a seu favor, visto que a cada vez mais "há uma possibilidade real de que com o uso das tecnologias por parte dos criminosos precisamos ter mais policiais que dominem a lógica das tecnologias digitais" (ALCADIPANI, 2020, p. 1).

Diante do cenário da necessidade de expansão do uso das TICs nas políticas públicas, o Estado, através do Governo Federal, desenvolveu planos de desenvolvimento das políticas de segurança pública, com a previsão de "melhorar a governança do setor público, aumentando a eficiência e eficácia das ações de governo" (BRASIL, 2018f, p. 20) se utilizando das tecnologias no combate à criminalidade como mais uma tentativa de melhorar a qualidade da segurança pública no Brasil.

3.1 PLANOS DE DESENVOLVIMENTO DAS POLÍTICAS DE SEGURANÇA PÚBLICA COM UTILIZAÇÃO DA TECNOLOGIA NO BRASIL

Para consecução da proteção da segurança pública, o Estado brasileiro deve propor, implementar e avaliar políticas públicas. Para Bucci (2006, p. 39), a política pública:

> é o programa de ação governamental que resulta de um conjunto de processos juridicamente regulados – processo eleitoral, processo de planejamento, processo de governo, processo orçamentário, processo legislativo, processo administrativo, processo judicial – visando coordenar os meios à disposição do Estado e as atividades privadas, para a realização de objetivos socialmente relevantes e determinados.

O PNS de 2000 (BRASIL, 2000) é considerado a primeira política de segurança pública brasileira focada no estímulo à inovação tecnológica. O PNS de 2000 previu a integração de políticas de segurança, sociais e ações comunitárias como medida importante para o aperfeiçoamento da segurança pública no Estado democrático de direito (LOPES, 2009), bem como o objetivo de reprimir e prevenir a criminalidade no Brasil.

De 2003 a 2017 foram instituídos outros programas[6] e políticas de segurança pública, com o escopo de articular ações policiais e da justiça criminal, restaurar a ordem pública e a

[6] Em 2004 ocorreu a criação da Força Nacional de Segurança Pública; em 2007 foi criado o Programa Nacional de Segurança com Cidadania (PRONASCI) com o objetivo de promover o financiamento de ações de prevenção

incolumidade física e patrimonial das pessoas, a exemplo da criação da Força Nacional, em 2004, e o estimulo de que financiadoras de projetos de inovação incentivassem a pesquisa de projetos relativos à aplicação da tecnologia à segurança pública.

Importante trazer à baila que, entre 2002 e 2010, a Financiadora de Estudos e Projetos (FINEP), principal agência de apoio a projetos de inovação no Brasil, financiou 53 projetos relativos ao desenvolvimento da segurança pública, dos quais 34 se referiram ao desenvolvimento de TICs, predominando o desenvolvimento de softwares para treinamento e identificação, radares e antenas (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2013).

Dentro do estímulo à inovação foi publicada a Lei nº 12.258/2010 que modificou a Lei de Execuções Penais e promoveu a possibilidade de utilização de equipamentos de vigilância pelos condenados pela justiça – monitoração eletrônica – para as hipóteses de saída temporária no regime semiaberto e cumprimento de pena em regime domiciliar. Em 2011, foi publicada a Lei nº 12.403, que modificou o Código de Processo Penal e instituiu o monitoramento eletrônico como medida cautelar no art. 319, inciso IX (VIDAL, 2014).

O monitoramento eletrônico consiste em condutas rastreadas via satélite que utiliza a radiofrequência e informações com criptografia de dados sobre o local onde se encontra o monitorado:

> No monitoramento eletrônico de condutas, o usuário é rastreado via satélite através de um aparelho chamado Sistema de Acompanhamento de Custódia 24 horas - SAC 24, que funciona através de rádio frequência e informações criptografadas dos dados sobre a posição em que se encontra o usuário. Os dados colhidos pelo sistema são enviados a um servidor e podem ser acessados por um terminal conectado à *internet*. O controle pode ser realizado através do uso de um bracelete, pulseira ou tornozeleira. O dispositivo utilizado pelo usuário possui um sensor antifraude e ruptura e possui uma bateria que dura em média 12 horas. Existe uma outra forma de monitoramento através de um *microchip* desenvolvido por nanotecnologia e que seria inserido no corpo do apenado, sendo os dados deste *chip* transmitidos via satélite, para que se saiba sua localização exata. (FIGUEIRA, 2008; VIDAL, 2014, p. 49, grifo do autor).

Para os defensores do monitoramento eletrônico, a tecnologia se apresenta como fator importante para a redução da população carcerária, diminuição dos gastos públicos com presos e reinserção no convívio social (GRECO, 2011; CARVALHO, 2010; VIDAL, 2014). O Superior Tribunal de Justiça (STJ), em decisão de 2011, se manifestou favorável quanto à

---

a violência; em 2012 foi lançado o Plano Brasil Mais Seguro, que apresentou como objetivo a redução da criminalidade violenta no país; em 2015 foi anunciado o Plano Nacional para Redução de Homicídios (PNRH). (BRASIL, 2018f, p. 34).

legalidade do monitoramento eletrônico e ainda decidiu a vantagem do equipamento – tornozeleira ou pulseira eletrônica – substituir a vigilância policial.

Por outro lado, há argumentos contra o monitoramento eletrônico, tais como possibilidade de retorno a um Estado totalitário, em que a sociedade seria a própria prisão, bem como estigmatização social da pessoa em razão da utilização do equipamento de monitoramento em público e ainda violação ao direito a intimidade e privacidade (KARAN, 2007).

Em 2012, foi publicada a Lei nº 12.681, que criou o Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas (SINESP), um sistema de TICs que se utiliza de uma plataforma de informações integradas das bases de dados do Governo Federal e dos estados, com o escopo de criar uma estrutura de gestão de informações em nível nacional, com a finalidade de produzir, coletar, sistematizar e disponibilizar informações para a segurança pública (SANTOS; LIMA; SOUZA, 2020).

Uma crítica ao SINESP é abordada por Santos, Lima e Souza (2020, p. 17) quando afirma que "a construção de um sistema que, por disposição legal, necessita da participação ativa de todas as unidades da Federação encontra de pronto um grande obstáculo inicial: diferentes realidades culturais, técnicas, metodológicas e orçamentárias" e recomenda em seu trabalho a sistematização da base de dados de forma mais integrativa e interoperável, se utilizando de inteligência operacional.

Ainda, em 2012, o Ministério da Justiça, com o objetivo de otimizar recursos públicos, de forma a desenvolver ações de fomento para ações de segurança pública, publicou o Edital Público 2012 e forneceu um guia de apresentação de propostas para o desenvolvimento de convênios do governo federal com os estados e municípios. No guia continha informações de como captar recursos do Fundo Nacional de Segurança Pública, nas ações de prevenção da criminalidade, com destaque para implantação ou expansão do videomonitoramento no país. Esse guia se transformou em um marco para o desenvolvimento do videomonitoramento no Brasil, visto que passou a destinar recursos para tal finalidade (FREITAS FILHO, 2018).

Em 2018 foi publicado o Plano Nacional de Segurança Pública de Desenvolvimento Social (PNSP) 2018-2028 (BRASIL, 2018f), criado pela Lei nº 13.675/2018, regulamentada pelo Decreto nº 9.489/2018, e que teve como escopo criar o Sistema Único de Segurança Pública (SUSP) para desenvolvimento de governança, "através da padronização de dados, integração tecnológica, de inteligência e operacional" (BRASIL, 2018f, p. 8), um marco no desenvolvimento e estímulo tecnológico.

Os objetivos previstos no SUSP foram o estabelecimento de princípios e estratégias da atuação do Estado na segurança pública com controle, transparência e prestação de contas. Uma importante previsão, visto a necessidade de *accountability* das ações do poder público (BRASIL, 2018f).

Ainda em 2018, o Conselho Nacional de Justiça (CNJ) criou o Banco Nacional de Monitoramento de Prisões (BNMP), base de dados em que constam os dados cadastrais das pessoas presas no sistema carcerário do Brasil, com o objetivo de centralização das informações e contribuição para o acesso às informações pelas autoridades judiciárias e policiais (SANTOS; LIMA; SOUZA, 2020).

O BNMP 2.0 "é um sistema eletrônico que auxilia as autoridades judiciárias da justiça criminal na gestão de documentos atinentes às ordens de prisão/internação e soltura expedidas em todo o território nacional, materializando um Cadastro Nacional de Presos" (SANTOS; LIMA; SOUZA, 2020, p. 10).

Em setembro de 2021, através do Decreto nº 10.882/2021, foi publicado o PNSP 2021-2030 (BRASIL, 2021c). Esse plano é constituído de objetivos, ações estratégicas, metas, sistema de governança e orientações aos entes federativos (artigo 1º, §2º).

São objetivos do PNSP 2021-2030: definir ações estratégicas, metas e indicadores para a efetivação do plano; determinar ciclos para implementação, monitoramento e avaliação da política; estabelecer estratégias de governança e de gerenciamento de riscos e ter papel de orientação aos demais entes federativos[7].

Dentre as ações estratégicas do PNSP 2021-2030, percebe-se o intuito do legislador em promover a expansão tecnológica na promoção de políticas de segurança pública, deixando claro a estratégia de padronização, integração e interoperabilidade dos dados sobre segurança pública entre União, estados, Distrito Federal e municípios.

Uma questão a ser destacada, é o fomento à utilização de ferramentas de *Machine learning* para categorização e análise dos dados, através da implementação do SINESP do sistema penitenciário nacional e por meio do sistema nacional de trânsito.

Destaca-se que o PNSP 2021-2030 apresentou os requisitos necessários para se concretizar a estratégia nº 7:

> a) Padronizar, integrar, coletar e consolidar dados e informações de interesse da segurança pública e defesa social, para o tratamento, a análise e a divulgação estatística; b) Promover a modernização e a interoperabilidade dos sistemas de

[7] Artigo 2º e incisos do Decreto 10.882/2021 que instituiu o PNSP 2021-2030.

> interesse da segurança pública e defesa social com vistas à integração, à gestão, à análise e ao compartilhamento de dados e informações; c) Integrar e aprimorar a base de dados entre os órgãos integrantes do SNT e os demais órgãos de segurança Pública e defesa social; e d) Ampliar os mecanismos de proteção e segurança de dados. (BRASIL, 2021c).

De igual modo, a estratégia nº 8 do PNSP 2021-2030 também prevê o fomento ao fortalecimento das atividades de inteligência nas instituições de segurança pública e defesa social, por meio de atuação do SUSP, com o objetivo de analisar, gerir e compartilhar dados e informações:

> a) Promover ações com o objetivo de dotar as instituições de segurança pública com ferramentas de inteligência modernas, padronizadas e integradas para a produção de conhecimento, em conformidade com a legislação aplicável; b) Atuar na estruturação e no aperfeiçoamento das atividades de inteligência penitenciária; c) Estimular a cooperação e o intercâmbio de informações de inteligência de segurança pública com instituições estrangeiras congêneres; d) Promover a criação e a estruturação da atividade de inteligência de trânsito; e) Integrar os sistemas e os subsistemas de inteligência de segurança pública e promover o compartilhamento de tecnologias interagências; e f) Estimular a articulação e a cooperação entre o sistema de inteligência de segurança pública com setores de inteligência da iniciativa privada, em conformidade com a legislação aplicável à proteção de dados. (BRASIL, 2021c).

Em 2021, ganhou destaque a adoção de câmeras corporais nos uniformes dos policiais, como política de segurança pública, também chamada de câmeras *body-worn*, que são como pequenas câmeras de vídeo, instaladas na farda, capacete ou óculos dos policiais, que tem a capacidade de captar e gravar, do ponto de vista dos policiais, vídeo e áudio das atividades desenvolvidas por eles em sua rotina policial, a exemplo de gravações de trânsito, detenções, revistas, interrogatórios, tanto no uso da força quanto na redução de queixas externas a atuação dos agentes (ALBARDEIRO, 2020).

O estado de São Paulo foi pioneiro na adoção da prática e replicada em outros estados como o Rio de Janeiro e Santa Catarina. Sob a ótica da sociedade civil, as imagens podem servir para garantir a disciplina e evitar o abuso de autoridade e os oficiais que defendem o projeto afirmam que as câmeras proporcionam segurança aos agentes (DUARTE, 2022). O dispositivo eletrônico acoplado as fardas funcionam da seguinte forma:

> O dispositivo é designado a um só agente, que precisa desbloqueá-lo com reconhecimento facial; O sistema reconhece o policial e solta a câmera, que já começa a gravar e a transmitir para o Centro de Comando e Controle; A autonomia do aparelho é de 12 horas; Por padrão, o aparelho grava em média resolução, e as imagens ficam armazenadas por 60 dias; Há a possibilidade, porém, de ativar o modo HD: nesse caso, as imagens são registradas em alta definição e ficam salvas em uma nuvem por até um ano; Tanto o policial em ação quanto o agente que estiver acompanhando do

> Centro podem acionar o HD; Os órgãos de controle, como as corregedorias, a Defensoria e o Ministério Público, poderão pedir as imagens. (G1 RIO, 2022).

Alcadipani (2021), quando questionado sobre o uso das câmeras nas fardas dos policiais, afirmou que "os resultados são positivos para a profissionalização da polícia, com redução da letalidade e preservação de provas nas ações policiais". Ainda se destaca um estudo realizado na análise da Polícia Militar de São Paulo que constatou que com a utilização das câmeras acopladas a farda dos policiais chegou a zero os homicídios nas áreas pesquisadas e foram aferidos baixos índices de lesão corporal (PAGNAN, 2021). Ainda os defensores dessa política se baseiam entre outros argumentos, no aumento da transparência e da legitimidade policial, coleta de provas, formação dos policiais, resolução célere de queixas (ALBARDEIRO, 2020).

Por outro lado, a política pública de acoplamento das câmeras nas fardas dos policiais também é questionada quanto ao argumento de violação da privacidade dos cidadãos, privacidade dos policiais, consequências indesejadas, com gravação de momentos constrangedores que podem intimidar policiais e a própria vítima que podem inibir algumas abordagens (ALBARDEIRO, 2020).

Diante da análise dos planos nacionais de segurança pública, no aspecto da promoção de políticas pública de segurança com o envolvimento da tecnologia, percebe-se um avanço no estímulo à inovação importante para a sociedade ao longo das últimas duas décadas, contudo, para Abramovay (2011 *apud* FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2013), como forma de ampliar a eficiência da promoção de tecnologias como políticas de segurança pública, o ideal seria que o Estado conseguisse estabelecer as reais necessidades de aplicação da política e a partir daí fossem recomendadas tecnologias específicas, uma vez que, para Abramovay (2011 *apud* FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2013), a habilidade para se identificar as áreas prioritárias das políticas de fomento tem se mostrado escassa.

Uma aliada tecnológica para o desenvolvimento de políticas públicas de segurança mais personalizadas e eficientes no combate à criminalidade é a IA. Essa personalização pode resultar em um resultado prático de formulação e implementação de políticas públicas, com maior integração entre homem/máquina. Ressalta-se, entretanto que a utilização da IA na segurança pública não é pacífica, visto que apresenta vantagens (ALCADIPANI, 2020; PAGNAN, 2021; DUARTE, 2022), mas também críticas quanto a possíveis violações de direitos fundamentais (SILVA, T., 2020a; NORRIS; ARMSTRONG, 1999; SOLOVE, 2011b).

A partir de agora, o presente trabalho se dedicará a tratar especificamente sobre IA, de forma que se torna necessário compreender o desenvolvimento da IA e sua implementação como política pública. Em razão da limitação do estudo, cumpre esclarecer que o recorte na abordagem da IA será norteado para o desenvolvimento e utilização do RF biométrico como política de segurança pública.

3.2 RECONHECIMENTO FACIAL COMO POLÍTICA DE SEGURANÇA PÚBLICA E SUA EVOLUÇÃO PARA A UTILIZAÇÃO DA INTELIGÊNCIA ARTIFICIAL

Ao se falar em tentativa de reconhecer uma pessoa, diversas técnicas podem ser empregadas, com destaque para as técnicas de identificação e RF na segurança pública para identificação de suspeitos de cometimento de crimes.

Desde o Egito antigo já se aplicavam técnicas de identificação dos indivíduos para extração de suas características, através da catalogação de marcas e cicatrizes das pessoas (MELO; NEVES; OLIVEIRA NETO, 2021, p. 131).

O Código de Processo Penal Brasileiro de 1941, em seu artigo 226, previu a possibilidade da utilização do reconhecimento de pessoas e objetos para investigação criminal. Para tanto, estabeleceu algumas regras para utilização, tais como as que a pessoa quem irá realizar o reconhecimento deverá descrever a pessoa a ser reconhecida e, se possível, a colocação da pessoa a ser reconhecida com outras que tiverem semelhança.

No Brasil também é admitido o reconhecimento de pessoas mediante o reconhecimento fotográfico de suspeitos em que supostos autores de crimes têm suas características físicas comparadas a um banco de imagens já existente nas bases da segurança pública (NUNES et al, 2016); por sua vez, o Supremo Tribunal Federal (STF) já decidiu que o reconhecimento fotográfico de suspeitos deve seguir a mesma regra do reconhecimento pessoal e ainda como fase anterior a este. Ainda o STF tem entendido pela nulidade do processo penal que resultou em condenação do acusado cuja prova exclusiva foi o reconhecimento fotográfico[8].

Uma técnica também utilizada para o reconhecimento de suspeitos é a representação facial humana ou retrato falado, uma vez que "por meio do relato de vítimas e testemunhas, e também de fotos e imagens se permite estabelecer a progressão da idade ou reconstituição facial" (SÃO PAULO, 2021, p. 1), através de desenhos manuais ou ainda pela utilização de softwares realizados por especialistas das polícias.

[8] Decisão do STF no Recurso Ordinário em sede de Habeas Corpus nº 206.846 – SP, 2021.

No ano de 2002 foi desenvolvido um sistema de reconhecimento, via retrato falado, denominado *fotocrim,* em que se utilizou como base de análise, o banco de dados de fotos digitais, disponível na Secretaria de Segurança Pública do Estado do Rio de Janeiro (SSP-RJ). O sistema inovava, tendo em vista a capacidade de inclusão de características étnicas da população brasileira (NUNES et al, 2016).

Quando da finalização da imagem, via retrato falado do suspeito, realizada mediante as características informadas pelo informante, a imagem é mostrada a ele e será considerada válida para continuidade da investigação nas delegacias se a imagem tiver um percentual de semelhança de pelo menos 60% com base no que o informante se recorda sobre a situação que ensejou a diligência policial (AMAZONAS, 2020).

Outra técnica para a utilização do RF remete ao registro de videomonitoramento por sistemas de CFTV, que é "um sistema em que um número de câmeras de vídeo está conectado em circuito fechado ou loop, com as imagens reproduzidas a serem enviadas por um monitor de televisão central e, ao mesmo tempo, gravadas" (GOOLD, 2004 *apud* ALBARDEIRO, 2020).

O registro mais antigo do CFTV ocorreu em 1942, na Alemanha, ainda na época do nazismo, através de uma tecnologia criada por Walter Brunch para monitorar o lançamento de foguetes (OLIVEIRA, 2021, p. 39).

Em 1947, contudo, ganhou destaque o videomonitoramento para efeito de segurança pública na Inglaterra, ocorrido em razão do casamento real e, em 1953, na coroação da Rainha Elisabete II. O videomonitoramento para vigilância foi abolido poucos anos após, em razão do grande índice de erros no reconhecimento, em razão das limitações das tecnologias das câmeras à época (OLIVEIRA, 2020).

Segundo Bonamigo, Pedro e Melgaço (2016), os dispositivos de controle e vigilância funcionam através de uma tecnologia híbrida, compreendida como uma rede sociotécnica, haja vista a vinculação entre diversas frontes, natureza-cultura, do científico, do político e do tecnológico em que há a troca de propriedades entre humanos e não-humanos.

O videomonitoramento transforma a ação humana para três deslocamentos: a) vetorial, em que as câmeras de monitoramento se tornam um personagem que produz efeitos; b) espacial, em que estes dispositivos ocupam espaços públicos e privados e c) temporal, visto que as câmeras estão presentes o tempo todo, inclusive substituindo a presença de policiais (BONAMIGO; PEDRO; MELGAÇO, 2016). Para Vilhena (2019), o CFTV apresenta diversas vantagens entre prevenção criminal, auxilio a investigação criminal, identificação de ofensores e testemunhas e a redução da sensação de insegurança pela população.

3.3 VIDEOMONITORAMENTO POR INTELIGÊNCIA ARTIFICIAL – RECONHECIMENTO FACIAL COMO POLÍTICA DE SEGURANÇA PÚBLICA

O presente tópico se dedicará a análise da utilização da IA e de que forma ela evoluiu para o desenvolvimento de softwares de RF, inclusive para aplicação como política de segurança pública.

Em 1955, o professor John MacCarthy utilizou o termo IA pela primeira vez em uma chamada para um projeto de pesquisa de Dartmouth College, EUA, cuja definição seria a capacidade da máquina realizar funções que, se realizadas pelo ser humano, seriam consideradas inteligentes (MCCARTHY, 2007).

Destaca-se, entretanto, que remete a Alan Turing, em 1950, o primeiro trabalho científico intitulado *Computer machinery and intelligence*, publicado na Revista *Psychology and Philosofy* em que foi explicitado a expressão: *machine intelligence*. Segundo Silva, S. (2020, p. 4), "A ideia de Turing dizia respeito à solução de problemas lógicos e matemáticos através da automatização em sistemas eletrônicos binários e a possibilidade de se construir máquinas capazes de aprender com a experiência" (SILVA, S., 2020, p. 4).

Muitos pesquisadores se esforçam para trazer a definição de IA, pois o conceito exato ainda é fonte de muitas discussões. Para Rosa (2011), uma definição bastante esclarecedora para IA é aquela apresentada por Rich e Night (1994 *apud* Rosa, 2011, p. 20): "[...] é o estudo de como fazer os computadores realizarem tarefas as quais, até o momento, os homens fazem melhor".

Já segundo Agrawal, Gans e Goldfarb (2019, p. 140), a IA é definida como "a teoria e o desenvolvimento de sistemas computacionais capazes de realizar tarefas que normalmente requerem a inteligência humana".

Schalkoff (1990) conceitua a IA no campo dos agentes racionais dos processos computacionais, de forma que seria um campo de estudo que busca explicar comportamentos inteligentes em processos de computação. A IA é formada por algoritmos que permitem a tomada de uma decisão automatizada a partir de fatores que são imputados pelo ser humano.

A IA pode ser aplicada para problemas que não tenham solução algorítmica, ou seja, "tarefas relacionadas com o processamento simbólico, reconhecimento de imagens e tudo que envolva o 'aprendizado'" (ROSA, 2011, p. 20, grifo do autor).

É papel da IA trazer o aprendizado do dia a dia para dentro das tecnologias, otimizando o tempo dos seres humanos e com a mesma excelência e, por vezes, maior que a realizada por

um humano, seu fundamento se baseia na ciência cognitiva, como filosofia, linguística, psicologia e ciência da computação (ROSA, 2011).

As ações do indivíduo, principalmente na internet, são monitoradas a todo instante, para que a IA se aproxime da realização de um perfilamento de interesses das pessoas de forma mais exata possível, de forma a ajudar as pessoas a encontrarem as opções dos produtos ou serviços que mais atendam às suas necessidades, bem como permitir que as empresas privadas e governos, através dos dados pessoais coletados, encontrem padrões para a realização de uma análise preditiva e assertiva na disponibilização dos serviços e produtos (PINHEIRO; FERRAZ, 2021).

O efeito social da criação de perfis das pessoas de forma tão preditiva, muitas vezes pode ser benéfica diante da exatidão dos resultados apresentados pela IA, haja vista o momento histórico-cultural representado pelo imediatismo onde não se pode perder tempo com aquilo que pode ser automatizado (PINHEIRO; FERRAZ, 2021), bem como pelo grau de assertividade algorítmica.

São exemplos de utilização da IA no contexto atual: a) análise de crédito realizada por instituições financeiras; b) análises preditivas de marketing digital para formação de perfil de consumo; c) realização de exames médicos com laudos de sugestão de patologias conduzidos por IA; d) construção de cidades inteligentes em que serviços são controlados pela IA – *smart city*; e) cirurgia por robótica e f) promoção de políticas públicas, a exemplo da disponibilização de aplicativos pelo poder público para programas sociais[9], utilização de robôs para análise de dados e a utilização do videomonitoramento com RF biométrico na segurança pública.

Para Kaufman (2018a, p. 29), "os algoritmos de aprendizado são os casamenteiros; eles encontram produtores e consumidores um para o outro com o melhor dos dois mundos; a diversidade de opções e o baixo custo da grande escala, com o toque da personalização associado aos pequenos", podem apresentar como efeito colateral a concentração de mercado para quem detém a tecnologia.

Ainda segundo Kaufman (2018a, p. 19), a IA "propicia a simbiose entre o humano e a máquina ao acoplar sistemas inteligentes artificiais ao corpo humano", a exemplo das próteses, fato este que Kaufman (2018a, p 19) também nomeia através da interação *homem/máquina*, *homem-aplicativos, homem-algoritmos* de IA. O homem é ao mesmo tempo gerador e consumidor de dados (SIQUEIRA; LARA, 2020).

[9] Auxílio Emergencial, Conect SUS, Carteira Nacional de Habilitação (CNH) digital, E-título do Tribunal Superior Eleitoral (TSE), etc.

A partir de 2010, surgiram diversas pesquisas sobre IA que, segundo Oliveira (2021), foram movidas pelos seguintes fatores:

> criação de métodos estatísticos e probabilísticos cada vez mais sofisticados; a disponibilidade de ampla e crescente quantidade de dados; acessibilidade a um enorme e relativamente barato, poder computacional; e a transformação, cada vez maior dos ambientes com as novas tecnologias de informação, como a automação residencial e a criação de cidades inteligentes. Tais fatores que se retroalimentam, possibilitaram o crescimento exponencial da criação e aperfeiçoamento dos sistemas de IA nos últimos anos, não aparentando ser uma tendência passageira. (OLIVEIRA, 2021, p. 42).

Assim, a IA, ao tratar grande quantidade de dados – *Big Data,* estruturados ou não, pode determinar padrões e prever eventos futuros até então desconhecidos, por meio de análise preditiva, que ajuda na identificação da probabilidade dos resultados (MAGALHÃES; VENDRAMINI, 2018).

Dessa feita, concluem os autores que "o crescimento exponencial dos dados inviabiliza a programação tradicional, remetendo inevitavelmente às técnicas de aprendizado de máquinas" (SIQUEIRA; LARA, 2020, p. 305). Dentre tais técnicas, destacam-se: *Machine learning,* terminologia criada por Arthur Lee Samuel, em 1959*; Deep learning* e Processamento de Linguagem Natural (PLN).

As diferenças entre as três técnicas de aprendizagem de máquinas residem no *modus operandi* da programação. Enquanto na técnica *Machine learning* o aprendizado da máquina é feito com pouca programação, deixando a máquina aprender por conta própria a partir do banco de dados que a alimenta, na *Deep learning* a máquina recebe um conhecimento profundo, com uma programação mais complexa a partir de algoritmos que imitam o cérebro. Já a técnica PLN busca por padrões em um grande conjunto de dados para realizar análise preditiva (MAGALHÃES; VENDRAMIINI, 2018).

Em se tratando de fundamento, a IA se baseia nos seguintes: a) redes neurais artificiais; b) sentido de noção de imitação; c) poder do automatismo e d) níveis tipológicos (SILVA JUNIOR, 2020). Por redes neurais artificiais pode se compreender "como uma composição de algoritmos inspirados nas estruturas e no modo de funcionamento de um neurônio biológico" (SILVA JUNIOR, 2020, p. 230). Nesse aspecto estão previstas a *Machine learning* e *Deep learning.*

No que concerne ao sentido de noção de imitação, com a aplicação da *Machine learning* os algoritmos passam a ter capacidade de não somente identificar padrões, mas de repeti-los. "Imitar é conservar e reforçar algo pré-existente" (SILVA JUNIOR, 2020, p. 230), o que pode

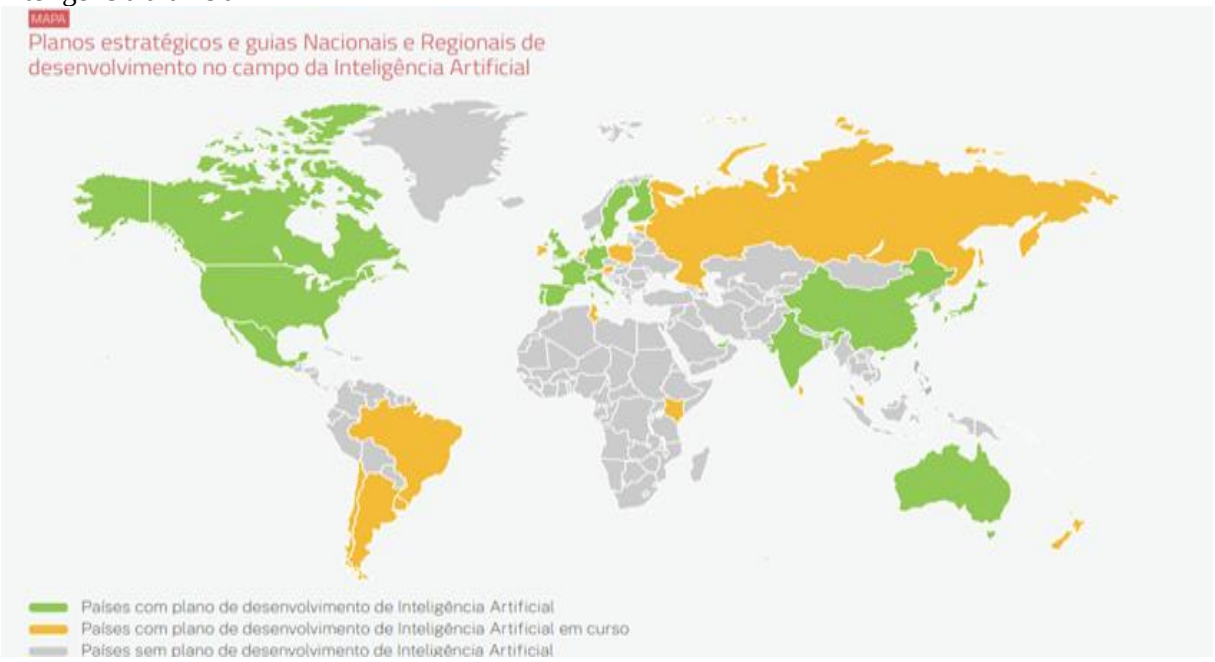
ser entendido como um paradoxo entre inovação e conservadorismo dos algoritmos de aprendizagem.

Por sua vez, o automatismo é um elemento fundamental, visto que a atribuição conceitual de inteligência da máquina é justamente o conseguir funcionar de forma autônoma, a partir de um *start* inicial (SILVA JUNIOR, 2020).

Por fim, o quarto elemento, níveis tipológicos, se refere ao grau de desenvolvimento da IA. O primeiro nível é o desenvolvimento de tarefas simples – IA Estreita, o segundo nível se refere a realização de tarefas simultâneas de forma parecida com o cérebro humano – IA Geral e o terceiro seria o nível de superação da inteligência humana – Superinteligência Artificial e que dependeria de processadores muito potentes e tecnologia quântica, o que ainda não se desenvolveu na sociedade atual (SILVA, JUNIOR, 2020).

Diversos países do mundo vêm cada vez mais se aprofundando na pesquisa quanto ao desenvolvimento da IA com ênfase na ampliação das atividades das indústrias, futuro do trabalho, políticas públicas e até controle social. Através de um levantamento realizado pelo Instituto de Tecnologia e Sociedade do Rio (ITS Rio) em 2019, assim se apresentada o mapa múndi com os países que apresentavam Planos Estratégicos e Guias Nacionais ou regionais de desenvolvimento da IA, representado pela Figura 1:

Figura 1 – Planos estratégicos e guias nacionais e regionais de desenvolvimento no campo da inteligência artificial



Fonte: ITS (2020).

A título exemplificativo, destacam-se no mundo os planos de estratégia da IA da China e da Comissão da União Europeia (UE), contemplados no relatório sobre IA realizado pelo ITS Rio, em 2020:

> **China:** Objetivo Estratégico Principal: O Plano estratégico chinês é bastante compreensivo e detalhado. Tem sua implementação prevista em três fases, com o objetivo de tornar a China líder mundial em IA até 2030. O primeiro passo é alinhar a indústria de IA da China com os concorrentes até 2020; o segundo, alcançar a "liderança mundial" em alguns campos de IA até 2025; e terceiro, tornar-se o centro "primário" da inovação em IA até 2030.
> **Comissão da União Europeia**: Objetivo Estratégico Principal: Desenvolver a pesquisa e a indústria europeias para colocar a IA a serviço da economia e dos cidadãos europeus. A abordagem europeia para IA é baseada em três pilares: 1) estar à frente dos desenvolvimentos tecnológicos e incentivar sua apropriação pelos setores público e privado; 2) preparar a sociedade para as mudanças socioeconômicas provocadas pela IA; e 3) implementar um Plano Coordenado de Inteligência Artificial "Made in Europe". A Comissão desenvolveu, juntamente com os Estados-Membros, um plano coordenado para IA, apresentado em dezembro de 2018, para criar sinergias, reunir dados — a matéria-prima de muitas aplicações de IA — e aumentar os investimentos conjuntos. (ITS, 2020, p. 15, grifos nossos).

A maioria dos países com estratégias de utilização de IA "utilizam para a transformação do setor público por meio da IA ou têm foco no setor público dentro de uma estratégia mais ampla" (BRASIL, 2021b, p. 43). Ainda, a Estratégia Brasileira de Inteligência Artificial (EBIA) (BRASIL, 2021b) destaca que essas estratégias utilizam questões centrais:

> - Colaboração entre diferentes setores, inclusive por meio de parcerias público-privadas, facilitada por hubs e por laboratórios de inovação.
> - Criação de conselhos, redes e comunidades envolvendo diferentes áreas do governo.
> - Automação de processos rotineiros para aumentar a eficiência.
> - Uso de IA para apoiar processos de tomada de decisão.
> - Gestão estratégica e abertura de dados governamentais, inclusive para alavancar IA no setor privado.
> - Orientações quanto ao uso transparente e ético de IA no setor público. (BRASIL, 2021b, p. 43).

Dada a velocidade de evolução da IA, pesquisadores tem questionado se ela poderá se tornar mais poderosa que os seres humanos. Para o professor Russel da Universidade da Califórnia, Berkeley, EUA, essa possibilidade existe, tendo em vista os grandes avanços tecnológicos, a exemplo dos carros autônomos, resolução de problemas de raciocínio lógico, percepção visual e na aprendizagem (RUSSEL; NORVING, 2013).

Contudo, Siqueira e Lara (2020, p. 304), quanto aos riscos, por sua vez, afirmam que "predizer os desdobramentos causados pela quarta revolução industrial na individualidade que

cerca a vida humana é algo que intriga pesquisadores do mundo remetendo-os, por vezes, a utopias e distopias que tornam a questão ainda mais intrigante", pela relação desenvolvida de uma relação homem/máquina marcada por uma tecnologia capaz de ser desenvolvida para se comparar com a inteligência humana.

Dentro das tecnologias que se utilizam da IA, se destaca o RF que são as habilidades que softwares de computados possuem de analisar rostos humanos constante de uma base de dados específica, se utilizando de conexões de internet para catalogar indivíduos, via captação de sua biometria extraída por smartphones, computadores e câmeras de vigilância (COSTA; OLIVEIRA, 2019).

A análise de múltiplos dados pessoais, até mesmo sensíveis, como a voz, biometria facial, das mãos, dedos e da íris, depois que coletados, são tratados pela IA para se tornarem um algoritmo, criar padrões dos indivíduos e, a partir daí, possibilitar a sua identificação e comparações com maior assertividade dos resultados da tecnologia (ARAUJO; CARDOSO; PAULA, 2021).

É importante destacar que por biometria entende-se "o reconhecimento automatizado de indivíduos com base nas suas características biológicas, como impressões digitais, formato do rosto, voz e íris ou comportamentais como jeito de andar ou falar" (ARAUJO; CARDOSO; PAULA, 2021, p. 2). A identificação biométrica atualmente conta com a classificação: sistema de identificação digital; sistema de identificação de íris; DNA; face e reconhecimento de voz (NUNES et al, 2016).

Os sistemas biométricos se dividem em dois grandes grupos: os invasivos "que necessitam da colaboração do sujeito para a sua identificação e os 'não invasivos' que podem ser utilizados até mesmo sem o conhecimento do identificado". O RF é um meio invasivo porque não muitas vezes a pessoa nem sabe que está sendo reconhecida pela IA (MELO; NEVES; OLIVEIRA NETO, 2021, p. 131, grifo do autor).

Conforme explica Franqueira, Hartmann e Silva (2021, p. 173-174), o RF atua primeiro com detecção da face, que será padronizada e alinhada de acordo com as faces que já foram constantes no banco de dados processadas pelo algoritmo, com base em um dado biométrico imutável, em que serão analisados milhões de faces captadas automaticamente pela IA. Assim a padronização é importante, haja vista que esta característica será analisada por variações estatísticas. O algoritmo analisa as faces detectadas e atribui pontuações por semelhanças.

Essas imagens captadas devem possuir uma qualidade mínima para a efetivação de uma leitura pelo algoritmo dos pontos fiduciais de forma a evitar que aconteçam falsos positivos e negativos. Pontos fiduciais são "pontos de controle sobre um objeto que definem regiões

características com propriedades interessantes à detecção. No caso da face, características faciais" (RIBEIRO et al, 2012, p. 1).

O falso positivo ocorre quando "há diferença entre o detectado e o que se quer detectar, mas a máquina aponta como sendo coincidentes" e o falso negativo é o contrário, quando não há o reconhecimento de quem deveria reconhecer (ALVES, 2020, p. 30).

Para que seja possível atualmente o RF automatizado, os softwares de RF necessitam que seja informado quem é uma determinada pessoa para que seja reconhecida em outras fotos (ALVES, 2020), como ocorre na Figura 2:

Figura 2 – Reconhecimento facial

Fonte: Smith, B. (2018).

O RF atualmente é possível tendo em vista enormes bancos de dados nos quais as imagens são catalogadas. Uma vez realizada a captura das imagens dos rostos, seja por câmeras de videomonitoramento, circuito fechado de TV ou até mesmo de outras fontes, a exemplo das redes sociais, a biometria facial é extraída e os dados pessoais processados podem ser utilizados para inúmeras finalidades (OLIVEIRA, 2021, p. 43), mesmo sem consentimento das pessoas.

Por sua vez, se torna importante para fins de imagem ideal que o banco de dados das imagens possua qualidade em imagens feitas em ambientes controlados, a exemplo do banco de dados dos documentos oficiais de identificação civil do governo (ALVES, 2020).

Salienta-se que os softwares que realizam o RF são alimentados por pessoas que trazem suas experiências e seus vieses pessoais e, portanto, não haveria como dissociar a IA de

possíveis falhas e até mesmo práticas que possam decorrer em violação dos direitos das pessoas (ARAUJO; CARDOSO; PAULA, 2021).

Ademais, falhas ainda podem acontecer no caso de leitura errada pelos algoritmos da máquina ou ainda em razão de imagens sem nitidez e clareza captadas no banco de dados analisado (ALVES, 2020).

Como política pública no Brasil, o RF biométrico começou a ser estimulado e previsto dentro dos objetivos do PNS de 2018, quando da previsão dessa possibilidade de uso da tecnologia no objetivo/estratégia nº 8, uma vez que há a expressa menção de estímulo pelo Estado, da utilização de RF como política de segurança pública para fiscalização de fronteiras, divisas interestaduais, portos, aeroportos, rodoviárias e ferrovias (PNS, 2018, p. 57). Como já anteriormente mencionado, o Estado da Bahia foi pioneiro na implementação do RF como política de segurança pública em 2018.

A aplicação da TRF como política de segurança pública não é algo pacífico, com argumentos fortes tanto para aqueles que a defendem quanto para aqueles que são contra a sua manutenção, assim, no próximo capítulo, serão abordados e analisados os benefícios e limitações dessa política pública.

4 BENEFÍCIOS E LIMITAÇÕES DA INTELIGÊNCIA ARTIFICIAL DE RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA

Diante da exposição no capítulo anterior quanto a utilização da IA de RF como política de segurança, mister se torna compreender quais seriam os possíveis benefícios enumerados pela administração pública para sua adoção, bem como quais seriam as possíveis limitações que pudessem provocar impactos na sociedade.

Dessa maneira, o presente capítulo tratará inicialmente dos benefícios e posteriormente tratará de limitações técnicas, de acurácia e confiabilidade, bem como de um tema muito sensível que é a possibilidade de vieses raciais e sexistas nos algoritmos utilizados na composição da ferramenta e que podem impactar em seus resultados como política pública.

4.1 BENEFÍCIOS DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA

A constatação de a cada vez mais crescente violência na sociedade, seja através das relações sociais do cotidiano, do crime, da ação Estatal para o combate ao crime, compõe um cenário de medo e insegurança na população e impõe desafios na construção de políticas públicas mais eficientes no combate à criminalidade (ALCADIPANI, 2020).

Criminosos cada vez mais se munindo de armas pesadas e meios tecnológicos a seu favor, ao passo em que a segurança pública contando com equipamentos obsoletos e com déficit de pessoas para investigação e atuação, torna as ações dos agentes de segurança pública em extrema desvantagem (ALCADIPANI, 2020).

Um relatório sobre violência realizado em 2013 pela Organização das Nações Unidas para Crimes e Drogas já apontava o Brasil como um dos países mais violentos do mundo, sendo que, em mapeamento realizado pelo Laboratório de Análise de Violência da Universidade do Rio de Janeiro, em 2016, restou constatado que um de cada quatro homicídios no mundo acontece em apenas quatro países: Brasil, Venezuela, Colômbia e México. (LABORATORIO DE ANÁLISE DE VIOLÊNCIA, 2016).

Assim, o estímulo à utilização da tecnologia como aliada da segurança pública se tornou uma alternativa importante no combate à criminalidade. “O policial operacional do futuro, possivelmente precisará de menos fuzis e mais domínios das ferramentas tecnológicas” (ALCADIPANI, 2020, p. 1).

O avanço tecnológico fez como que fossem expandidas possibilidades de adoções de técnicas para o controle estatal, tais como escutas telefônicas, gravações ambientais,

intercâmbio de dados, rastreamento por dispositivos eletrônicos e a vigilância através das câmeras de vídeo. Essas medidas, segundo Roxin (1997), são eficientes na prevenção e combate à criminalidade e não ferem nenhum direito constitucional, uma vez que a convivência social já pressupõe conviver sendo observado por outras pessoas.

A utilização do videomonitoramento na segurança pública visa proporcionar aos cidadãos mecanismos mais ágeis para resolução de incidentes e emergências, de forma a consolidar a aplicação do princípio da universalidade, na medida em que "serão realizados o recebimento de todas as chamadas e solicitações dos cidadãos, designação de recursos mais eficientes para a solução e seguimento integral das atividades policiais, a garantia aos direitos individuais e coletivos" (FREITAS FILHO, 2018, p. 72). O investimento em RF vai conferir muito mais resolutividade à segurança pública, segundo o secretário de segurança pública do Estado da Bahia em 2021, Ricardo Mandarino (RODRIGUES, 2021).

O princípio da universalidade integra o regime jurídico do serviço público:

> Tal instituto traduz-se em prestações materiais, titularizadas pelo Estado e prestadas por ele ou por quem lhe faça as vezes, sob um regime publicista. Mediante tais prestações, o Estado cumpre seu dever de realização dos direitos fundamentais sociais, plasmados na Carta Constitucional de 1988. Direcionado a tal desiderato, o princípio da universalidade assegura a todas as pessoas o acesso às prestações decorrentes dos serviços públicos, sendo dever inescusável do Estado permitir, a toda a população, o acesso às comodidades materiais decorrentes de tais prestações. Tal princípio traduz, assim, o dever de universalizar o acesso aos direitos fundamentais sociais concretizados mediante os serviços públicos prestados, manifestando-se como condição de realização dos objetivos fundamentais previstos no texto constitucional. (SCHIER, [2017], p. 1).

Assim, através do videomonitoramento, o princípio da universalidade também seria aplicado para outras situações que não somente de Segurança, tais como: emergência policial, saúde, defesa civil, bombeiros, grandes catástrofes, de um ponto integrado, que possibilitará informação e assistência a todos os entes públicos federais, estaduais e municipais que necessitem (FREITAS FILHO, 2018).

Freitas Filho (2018) conclui que a adoção do videomonitoramento foi traçada sob uma perspectiva de não discriminação para o pronto atendimento de qualquer cidadão e conclui afirmando que a vídeovigilância nas áreas urbanas de alta estatística criminal apresenta-se como uma medida apropriada para o exercício do policiamento.

Destaca-se que a persecução por novos modelos de gestão na segurança pública perpassou pela implementação de inovações tecnológicas e foram surgindo outras tecnologias mais eficientes e precisas, como o RF ao vivo, que aumentam a precisão no reconhecimento de pessoas e podem contribuir para localização de foragidos da justiça ou ainda de pessoas

desaparecidas, uma medida importante para efeitos de segurança pública (BAHIA, 2019h).

No Brasil, em junho de 2022, havia 330.849 pessoas que constavam no Banco Nacional de Mandados de Prisão do CNJ como procurados e mais 24.159 como foragidos da justiça brasileira (CNJ, 2022).

Dito isso, para os olhos humanos reconhecerem essas pessoas procuradas pela justiça em meio à sociedade, se torna uma missão muito difícil. Assim, com a ajuda do RF, a identificação desses foragidos pelos policiais pode ser realizada em poucos segundos, visto que são emitidas notificações para a polícia quando o criminoso passa pelas câmeras de segurança, como projeção que chega de informações em até dois segundos, para algumas tecnologias, como por exemplo, a ferramenta FindFace (NTECHLAB, 2022).

Um grande benefício da utilização do RF é quanto ao objetivo também de atuação preventiva das polícias na segurança de grandes eventos públicos, através da detecção de pessoas que possam representar ameaças à segurança pública, de forma rápida e eficaz (NTECHLAB, 2022).

Outra importante utilização que a TRF permite é a utilização dos dados coletados no RF como medidas de análise pela segurança pública sobre o fluxo de pessoas em locais públicos e suas características sociodemográficas. Dessa maneira, os dados coletados se tornam de extrema importância para a realização do planejamento de serviços operacionais e comunitários de gerenciamento estratégico das polícias nos locais analisados (NTECHLAB, 2022).

Tecnicamente, o videomonitoramento é adotado mediante os modelos de câmeras exemplificadas na Figura 3 que, localizadas em espaços públicos, contribuem para as ações da segurança pública da seguinte forma:

Figura 3 – Modelos de câmeras de videomonitoramento

Fonte: Instituto Igarapé ([2019 e 2021]).

No Reino Unido, um dos países pioneiros que utilizam o RF e que já chegou a mais de 6 milhões de câmeras de vigilância instaladas, um estudo do Instituto Lovelace, realizado em 2019, constatou o apoio popular ao RF pelas polícias. Destaca-se, por sua vez, que 55% das pessoas que acreditaram que o governo deveria impor limites ao uso da TRF. No embate entre "segurança" e "privacidade" a tendência é de que a segurança prevaleça (SOLOVE, 2011a).

Vale salientar que um outro estudo realizado pela London Policing Ethics Panel, pelo London Mayor's Office for Policing and Crime e pelo University College London Institute for Global City Policing, revelou que 57% dos entrevistados apoiavam o RF, contudo, quando se analisou o percentual em grupos minoritários, o número de oposição a RF pelas polícias foi maior, sendo 56% de pessoas asiáticas e 63% de oposição para pessoas negras, mas ainda assim um majoritário apoio popular.

Para Vidal (2014, p.43), o apoio popular a medidas de vigilância se destaca pela disseminação pelo Estado da **cultura do medo**, "através da exploração e divulgação da violência e os efeitos nefastos do sentimento de insegurança", como uma das mais importantes formas de controle estatal.

Já para o coronel Maurício Fliess, Coordenador de comunicação da Polícia militar do Rio de Janeiro, a aplicação do RF automatizado em massa implicará em redução da criminalidade; no mesmo sentido, Mauricio Barbosa, ex-Secretário de Segurança Pública do Estado da Bahia, destaca a importância para a área policial a obtenção de inteligências através das imagens para uma intervenção futura, se antever à criminalidade e há o destaca para a adoção de um política pública de segurança não letal (G1, 2019).

O uso do RF apresenta uma possibilidade extraordinária de melhoria na infraestrutura de segurança pública, desde que prescindindo de que observação dos mecanismos de controle ético, social e jurídico da tecnologia (OLIVEIRA et al, 2021).

Segundo Pablo Lira, professor do Mestrado em Segurança Pública da Universidade de Vila Velha - ES, a utilização do RF é bem-vinda, na medida em que "é uma ferramenta que atrela o banco de criminosos procurados com uma ferramenta que já está difundida nos grandes centros, que é o videomonitoramento" (PALMA; PACHECO, 2020) e, ainda pode ser apresentado como uma tecnologia que contribui na formação de provas (gravações) para serem utilizadas pelo Ministério Público e Poder Judiciário.

Ainda, a aplicação do RF na segurança pública permite que a política pública se torne flexível e com adoção de mobilidade, visto que os policiais, que estarão nas salas de controle analisando as imagens captadas, passam essas informações, em tempo real, para os policiais em campo mais próximos da ocorrência, sejam através de rádios, celulares ou até mesmo tablets

que contenham aplicativos do sistema e que farão a abordagem da pessoa identificada como criminoso foragido da justiça em pouco tempo (NTECHLAB, 2022).

Tecnologia de ponta sendo utilizado pela segurança pública no combate à criminalidade, o RF automatizado também apresenta benefícios para a administração pública com relação a redução de custos de pessoal e utilização de equipamentos públicos (TERMO..., 2019). As abordagens policiais às pessoas são mais direcionadas pela análise indicativa prévia da tecnologia, diminuindo o público a ser abordado para revista e tornando a abordagem policial mais criteriosa e eficiente.

Importante destacar que a segurança pública no Brasil, de forma geral, realiza a contração de empresas terceirizadas para a prestação dos serviços de RF, visto que há um déficit de mão de obra qualificada em áreas críticas em tecnologia para adoção e condução de novas políticas públicas inovadoras, além de longos prazos para compra de insumos e materiais, aquisição de equipamentos próprios e dos custos desse tipo de aquisições, o que poderia inviabilizar a promoção da política pública (BAHIA, 2019h).

Dessa forma, "a contratação de *outsourcing* da tecnologia reduz os custos operacionais, garante o recebimento de um serviço de melhor qualidade e, principalmente, propicia à organização manter o foco no negócio" (BAHIA, 2019h), sem se preocupar com custos de manutenção e operacionalização, sem interrupções por falta de peças ou ainda por falta de pessoal especializado (BAHIA, 2019h)

Com isso, esforços estão sendo agregados para a utilização do RF como construção de um modelo de política pública que confira a garantia de qualidade dos serviços prestados com benefícios ao interesse público e investimentos com custos menores com a prestação de serviços otimizada (BAHIA, 2019h, p. 4).

4.2 LIMITAÇÕES TÉCNICAS DA UTILIZAÇÃO DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA: ACURÁCIA E CONFIABILIDADE

Fato notório é o exponencial desenvolvimento da tecnologia, principalmente a partir da última década, contudo, por mais que o RF desenvolvido pela IA tenha avançado em suas características e aplicações, algumas questões técnicas ainda são entraves para o seu desenvolvimento, a exemplo da falta de precisão – acurácia (RUBACK; AVILA; CANTERO, 2021; OLIVEIRA, 2021; SILVA JÚNIOR, 2020).

A acurácia é uma métrica intuitiva para avaliação de desempenho dos modelos de aprendizado de máquinas, cuja aplicação se refere a consideração da proporção de acertos em

relação ao total (RUBACK; AVILA; CANTERO, 2021). Assim, a falta de acurácia pode ocorrer, por exemplo, em razão de um banco de dados com imagens ruins, sem nitidez e qualidade, ou ainda por problemas no desenvolvimento dos softwares através de falhas no desenvolvimento do *machine learning*, *deep learning* ou ainda na composição das redes neurais artificiais.

Nesse sentido, na aplicação de softwares de RF, destacam-se alguns casos emblemáticos de como a falta de acurácia pode implicar em violação de direitos humanos[10].

Um estudo da União Americana pelas Liberdades Civis (ACLU) comprovou a falta de precisão dos algoritmos na identificação no software Rekognition[11] quando realizado um teste com o reconhecimento dos rostos dos 535 Congressistas dos EUA, uma vez que em 28 deles houve falso-positivo no reconhecimento errôneo de parlamentares com pessoas que já haviam sido presas, ainda revelou uma predisposição maior de erros no reconhecimento de pessoas pretas, que chegou a 39% (OLIVEIRA, 2021; RUSSEL; NORVING, 2013).

O Rekognition teria como base a tecnologia de *deep learning*, com um aprendizado profundo e altamente escalável, desenvolvido pelos cientistas da computação da empresa para analisar bilhões de imagens e vídeos diariamente com precisão e confiabilidade da tecnologia (OLIVEIRA, 2021; SILVA JÚNIOR, 2020).

Para Jacob Snow, líder do estudo da ACLU, os possíveis erros e o comprometimento dos direitos humanos deveriam fazer com que o governo decretasse uma moratória sobre o uso do RF (RUSSEL; NORVING, 2013). A moratória aconteceu, em 2020, por iniciativa da própria da Amazon (2020) quanto a possíveis vieses e imprecisões do seu software de RF, haja vista a falta de regulamentação do governo para utilização dessa tecnologia, com a justificativa de potencial para violação a preceitos éticos e aos direitos humanos.

Em 2021, a Amazon (2021) baniu o Rekognition nos EUA, em razão de ainda não ter havido uma regulamentação legal, bem como pelo reconhecimento da empresa dos vieses raciais e da possibilidade do software ser utilizado para fins de vigilância em massa.

---

[10] O primeiro caso real de falha no software de RF aplicado na segurança pública ocorreu no Estado do Michigan, EUA, quando Robert Julian-Borchak Williams, um homem negro, foi preso por ter sido erroneamente reconhecido como autor de um furto a uma relojoaria. A tecnologia não estava apta a reconhecer rostos negros, visto que essa foi apontada como a única correlação entre Williams e o verdadeiro criminoso (OLIVEIRA, 2021, SILVA, T., 2020).

[11] A Amazon desenvolveu um software de RF denominado Rekognition. Esse software vinha sendo utilizado para fins de comparação de rostos, verificação de usuário e até segurança pública. O software foi utilizado pela polícia de São Francisco, Califórnia, Oregon e Flórida, todos nos EUA, para fins de segurança pública (OLIVEIRA, 2021).

Em janeiro de 2020, a polícia de Londres informou que passaria a utilizar o RF via IA em espaços públicos de grande movimento, fato que já vinha ocorrendo antes, mesmo sem a ciência das pessoas. O posicionamento do governo foi de um teste de 70% de êxito na identificação de suspeitos de crimes, sendo um alerta falso para cada 10 mil (SILVA, P., 2020).

Entretanto, um estudo da Universidade de Essex apresentou resultados diferentes, no sentido do RF biométrico em tempo real, utilizado pela Polícia de Londres, possuir uma taxa de acerto de apenas 19%. Das 42 pessoas analisadas pelo RF no estudo, apenas oito realmente estavam na base de dados do governo (OLIVEIRA, 2021; SILVA, P., 2020), o que chama atenção para a falta de acurácia e confiabilidade dos softwares.

Outro estudo realizado no Reino Unido, concluiu que a utilização do RF automatizado resultou em um índice de 95% de identificação incorreta de pessoas, de acordo com a base de dados de integração do sistema. O alto índice de falta de acurácia no sistema gera efeitos de falsos-positivos na atuação policial, comprometendo sua efetividade (ALMEIDA, 2022).

Por outro lado, cumpre destacar que o alto desenvolvimento das tecnologias está fazendo com que, cada vez mais, a acurácia seja aumentada no RF. Nesse esteio se destaca o software de RF, via IA desenvolvido pelo Serviço Federal de Processamento de Dados (SERPRO), principal provedor de soluções tecnológicas para o estado brasileiro, denominado Datavalid, que é uma técnica de visão computacional que utiliza redes neurais e em que, segundo informações da empresa pública, chegou a 99,99% de acurácia no RF realizados (SERPRO, 2020).

A alta acurácia da ferramenta, segundo a SERPRO (2020), foi possível por um conjunto de dois algoritmos, um original e um outro novo, que permitiu a dupla validação nos casos onde a probabilidade da incerteza no reconhecimento fosse maior. O Datavalid não é utilizado como ferramenta de RF para fins de segurança pública e se utiliza de bancos de dados oficiais do governo para identificação facial, o que já conteria um banco de imagens com imagens mais selecionadas.

Dito isso, um dos grandes desafios para se aumentar a acurácia dos softwares de RF na segurança pública e torná-la uma política pública mais eficiente, seja a utilização de um banco de dados com imagens unificadas, de boa resolução e com a viabilização de sua interoperabilidade entre os órgãos e instituições que compõem a segurança pública no Brasil, haja vista que hoje os bancos de imagens da segurança pública sejam conduzidos de forma descentralizada pelos governos estaduais (ALVES, 2020).

Além disso, é importante mencionar que os softwares também estão sujeitos a fraudes e vieses, o que pode comprometer a assertividade (OLIVEIRA, 2021). Segundo Hong (2020,

apud OLIVEIRA, 2021, p. 66), as pessoas tendem a ter uma "fé na objetividade da tecnologia", que seria uma autoridade inquestionável decorrente do progresso.

Assim, "a questão é que as limitações do conhecimento orientado por dados não residem nos limites da tecnociência, em si, mas sim nas consequências não intencionais dos algoritmos e da discricionariedade humana a qual é inevitavelmente enviesada" (OLIVEIRA, 2021).

4.3 VIESES DO ALGORITMO

Segundo Goulart e Timm (2020), o ser humano toma suas decisões de acordo com o sistema cognitivo 1 que permite tomar decisões rápidas, automáticas e intuitivas, sendo que nesse ponto se situam os vieses e as heurísticas cognitivas que estão mais sujeitas a erros, e com o sistema cognitivo 2 que se trata da tomada de decisões mais pensadas, racionais.

Os vieses podem ser entendidos como decisões, nem sempre racionais, baseadas em associações das experiências anteriores das pessoas, que podem apresentar preconceitos contra determinados grupos (RUBACK; ÁVILA; CANTERO, 2021, p. 5), "seria uma tendência do algoritmo em não modelar o problema de forma correta, ou não generalizar o suficiente, por não considerar os dados necessários" (SILVA JÚNIOR, 2020, p. 42).

Assim há dois cenários: ou as características da amostra não foram suficientes capturadas pelo modelo utilizado no treinamento dos algoritmos ou o conjunto de dados disponível para o treinamento não contém exemplos representativos do problema a ser resolvido. O cenário dois representa o viés de dados – *Data Bias* (SILVA JÚNIOR, 2020).

Com o desenvolvimento da IA, os algoritmos se tornam importantes para ajudar o ser humano nas tomadas de decisões. "De um modo geral, a tomada de decisão por algoritmos pode significar um meio de mitigar os vieses e as heurísticas cognitivas do ser humano e, por consequência, de evitar eventuais equívocos ou erros na realização de uma escolha" (GOULART; TIMM, 2020).

Com o uso das decisões algorítmicas de forma escalável, há uma tendência maior de delegação de tomadas de decisões mais racionais, muito pela confiança de que os robôs adotariam decisões com mais qualidade – fé na objetividade da ciência (HONG, 2020; GOULART; TIMM, 2020).

De fato, a IA pode reduzir a subjetividade que envolve decisões tomadas por seres humanos, pois os algoritmos de *machine learning* são treinados para considerar variáveis que aumentem suas precisões nas previsões, e esse treinamento melhora a performance das tomadas de decisões, a fim de que estas se tornem mais imparciais (SILBERG; MANYIKA, 2019). "Os

algoritmos extraem padrões, a partir de grandes bancos de dados, e são baseados em modelos estatístico" (RUBACK; ÁVILA; CANTERO, 2021, p. 5).

No entanto, exemplos ao longo da recente história demonstram o impacto do enviesamento na IA. Norris e Armstrong (1999) realizaram um estudo sobre os centros de monitoramento através de CFTV, na Inglaterra, que, em único dia, a pessoa, em Londres, tinha sido filmada por mais de 300 câmeras existentes no sistema de transporte, hospitais, estádios, ruas, etc. e constataram direcionamentos relativos a gênero, idade, raça e etnia, por exemplo, os negros apresentaram de 150% a 250% mais chances de serem abordados pela polícia do que as pessoas brancas, o que afetaria o posicionamento de neutralidade e imparcialidade.

Os algoritmos enviesados – *Biased algorithms* podem ocorrer em razão de transmutarem com a precisão o treinamento de modo e critérios estabelecidos pelo programador que o criou ao imputar ou retirar dados que reflitam sua forma de pensar na sociedade sobre questões como o racismo e desigualdades sociais. Assim, "os dados subjcentes e não os algoritmos em si costumam ser a principal fonte do problema" (SILBERG; MANYIKA, 2019, p. 1).

Ruback, Ávila e Canteiro (2021), afirmam que os vieses podem ser inseridos nos algoritmos desde a fase de coleta de dados, como, por exemplo, no RF em que alguns projetos são disponibilizados com dados de rostos para *download*, para serem utilizados nos treinamentos de dados e fase de pré-processamento que envolve a limpeza de dados incorretos, incompletos, criação de modelos que utilizam dados de treinamento, sem incluir dados de testes, a fim de que os algoritmos testem modelos com diferentes parâmetros e métodos para melhorar o desempenho (RUBACK; ÁVILA; CANTERO, 2021, p. 5).

Ainda, podem haver vieses na avaliação do modelo com aplicação de métricas para otimizar esses resultados e na fase de pós-processamento, uma vez que após a finalização do aprendizado da máquina devem ser feitos novos testes. "O processo de desenvolvimento de um modelo de aprendizado de máquina geralmente é incremental, de forma que eles são retroalimentados com feedbacks – sobretudo indicando os erros nas predições" (RUBACK; ÁVILA; CANTERO, 2021, p. 7).

Os vieses podem surgir em diversas etapas. Segundo Ruback, Ávila e Canteiro (2021, p. 6-7), podem ser exemplos de vieses os erros no RF de pessoas pretas (viés históricos), de gênero (viés por amostragem) e de diversidade da composição do banco de dados (viés de avaliação):

> Viés histórico: Os vieses históricos acontecem na etapa anterior à coleta de dados [...] Quando dados de entrada refletem na saída resultados passados, que podem ser

> discriminatórios, eles reforçam julgamentos e preconceitos dos indivíduos e instituições, como o racismo.
> Viés de representação (ou de amostra): Os vieses de representação podem acontecer na etapa de coleta de dados [...] e são incluídos na própria construção de dados de treinamento não representativos. Quando a amostra coletada não é representativa da população a ser modelada, de forma balanceada, o modelo irá errar muito mais em predizer rótulos para estes grupos sub-representados.
> Viés de avaliação. Os vieses de avaliação podem ser inseridos na etapa de avaliação do desempenho do modelo. O modelo aprende com os dados de treinamento, mas tem a sua qualidade avaliada a partir de dados de teste – ou de dados de referência [...] Dados usados como referência que não representam de forma balanceada os diferentes subgrupos da população [...] levam a modelos com vieses de avaliação. (RUBACK; ÁVILA; CANTEIRO, 2021, p. 6-7).

Para tentar resolver os problemas do enviesamento algorítimo, algumas técnicas estão sendo estudadas para tentar aumentar a explicabilidade das decisões da IA. A primeira consiste no pré-processamento de dados, "de forma a produzir representações dos dados que não contenham informações sobre atributos sensíveis" (SILBERG; MANYIKA, 2019), e a segunda consiste no pós-processamento, ou seja, depois de serem feitas as previsões, algumas delas serão transformadas para o alcance da imparcialidade (SILBERG; MANYIKA, 2019, p. 3).

Esses problemas ocorrem, como bem explicitado por Negri, Oliveira e Costa (2020, p. 3), tal como trazendo as ideias de Norris e Armstrong (1999) e Bioni e Luciano (2019), em razão da "falta de regulação, monopólios no setor de IA, assimetrias de poder entre empresas e usuários, a distância cultural entre os responsáveis por pesquisas em tecnologia e a diversidade das populações nas quais essa tecnologia é utilizada".

Ademais, a minimização dos vieses se torna de extrema relevância para a utilização da IA, assim o Silberg e Manyika (2019) enumera algumas condutas a serem consideradas por profissionais de IA, empresas e formadores de políticas, na forma descrita no Quadro 2:

Quadro 2 – Seis condutas possíveis a serem consideradas por profissionais de inteligência artificial, empresas e formadores de políticas

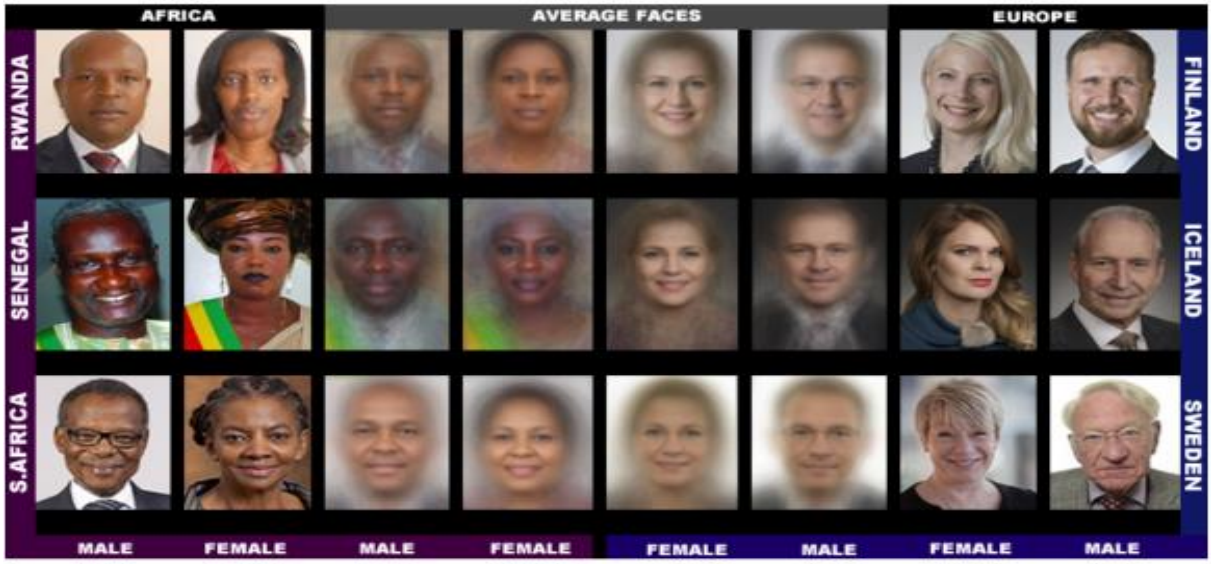
1	Estar consciente dos contextos em que a IA pode ajudar a corrigir vieses, bem como em que pontos há um alto risco de que a IA exacerbe viesses existentes.
2	Estabelecer processos e práticas para testar e atenuar o viés em um sistema de IA.
3	Ter conversas baseadas em fatos sobre os potenciais vieses de decisões humanas.
4	Explorar a fundo a melhor maneira de seres humanos e máquinas trabalharem juntos.
5	Investir mais em pesquisas sobre vieses, disponibilizar mais dados para pesquisa (sempre respeitando a privacidade) e adotar uma abordagem multidisciplinar.
6	Investir mais na diversificação do próprio campo de IA.

Fonte: Silberg e Manyika (2019), adaptado pela autora.

No Brasil, em razão da pluralidade étnica da população, pela miscigenação, apresenta dificuldade particular em relação a outros países no quesito qual o sistema algorítmico a ser utilizado para biometria facial (ALVES, 2020, p. 23), o que faz aumentar o cometimento de falhas de reconhecimento. “No mesmo sentido é importante compreender as formas como a vigilância é exercida, influenciada por preconceitos e padrões de dominação e gerando, ou pelo menos contribuindo, para a manutenção de determinada ordem social, demarcando fronteiras e segregando populações” (OLIVA, 2015, p. 139).

O estudo de Buolamwini e Gebru (2018) denominado Gender Shades, representado pela Figura 4, se tornou um marco quanto a sua relevância por apresentar questões polêmicas quanto aos vieses da IA raciais e de gênero quando da aplicação do RF. Como forma de diminuir os vieses, Buolamwini e Gebru (2018) apresentaram um Pilot Partiament Benchmark (PPB), um software alimentado com 1.270 imagens de rostos de parlamentares de três países africanos e três europeus, que continha equilíbrio entre gênero, cor de pele e fenótipo e o resultado foi um maior grau de assertividade na análise, o que demostra que o viés de avaliação pode ser minimizado, se utilizado uma base de dados mais diversa (RUBACK; ÁVILA; CANTERO, 2021, p. 7).

Figura 4 – Dados do software Pilot Partiament Benchmark



Fonte: Buolamwini e Gebru (2018).

Apesar dos avanços de técnicas que tem como escopo reduzir os vieses na IA, fato é que se torna uma tarefa muito difícil, de mudança de cultura social dos programadores e desenvolvedores da tecnologia, sobre questões tão sensíveis na história mundial como são o racismo e o sexismo que impactam nos resultados das políticas públicas, principalmente de segurança pública.

4.3.1 Racismo Algoritmo

O estudo de Norris e Armstrong (1999), apresentado no tópico anterior – 4.3 Vieses do algoritmo, foi o pioneiro na demonstração de possíveis vieses raciais nos algoritmos ao identificar a grande possibilidade de erros de RF para os negros, fazendo com que um algoritmo pudesse replicar preconceitos, tendo em vista a falta de diversidade dos programadores e o input de seus valores no algoritmo. (NORRIS; ARMSTRONG, 1999, p. 150).

Foi demonstrado que, quando se tratavam de homens, negros, a categorização de suspeitos se dava com base no pertencimento a um grupo social específico, dessa maneira, a persecução de democracia como desejo da tecnologia se transmutava para a vigilância daqueles grupos socialmente marginalizados (NORRIS; ARMSTRONG, 1999):

> Of course, it may be argued that since those officially recorded as deviant, are disproportionately young, male, black, and working class, targeting such groups merely reflects the underlying reality of the distribution of criminality. Such an argument is, however, circular: the production of the official statistics is also based on pre-given assumptions as to the distribution of criminality, which itself leads to the particular configuration of formal and informal operational police practice. As self-reports studies of crime reveal, offending is in fact, far more evenly distributed throughout the population than reflect in the official statistics. (NORRIS; ARMSTRONG, 1999, p. 150).

Por outro lado, para efeito de contribuição da pesquisa, há autores como Kleinberg (2018) que acreditam que os algoritmos podem reduzir as disparidades sociais no sistema de justiça criminal, haja vista a possibilidade de sua alta precisão e ainda imparcialidade.

Em 2009, um caso se tornou viral na internet quando duas pessoas, sendo um homem negro (Desi Crayer) e uma mulher branca (Wanda Zamen), estavam fazendo testes em frente a uma câmera Hewlett-Packard (HP) de RF no trabalho, mas a câmera, aparentemente, não conseguia localizar o rosto de Desi, somente o de Wanda. A situação gerou à época grande repercussão quanto a falha no reconhecimento de pessoas pretas, mas a HP se manifestou informando ter sido uma falha decorrente de baixa iluminação. Com o relato, diversas outras pessoas também notificaram a empresa quanto ao não reconhecimento dos rostos de pessoas pretas (SIMON, 2009).

Os vieses raciais também podem se fortalecer para efeitos de RF, na medida dos dados imputados por usuários do sistema, uma espécie de *loop* de *feedback*, por exemplo, quando da associação em sites de buscas realizadas com nomes de afro-americanos que tenderam a produzir mais anúncios com a palavra **detenção** (MCKINSEY, 2019).

Tarcízio Silva (2020) expõe que a tecnologia não é neutra, porque em seu resultado acaba por trazer valores das pessoas que a constroem e que, muitas vezes, trazem traços de racistas na transmutação dos códigos:

> Não se trata de algoritmos racistas ou apenas "enviesados" nas bases de dados e códigos, mas sim de racismo algorítmico: a intensificação da opacidade e da ignorância para a reprodução das desigualdades e estruturas de poder contemporâneas. Subjacente à lógica do aprendizado de máquina, o poder hegemônico estabelece que as decisões e dinâmicas sociais, comerciais e de gestão pública nos últimos anos estavam corretas e devem ser replicadas e reforçadas, com mais eficácia e opacidade, por sistemas algorítmicos. Abdicar da epistemologia da ignorância – tanto sobre a tecnologia quanto sobre o racismo – é indispensável para um futuro justo. (RFI, 2019, grifo do autor).

Em 2015, um caso de erro de algoritmos de RF da Google, no aplicativo Google fotos, teve muita repercussão, haja vista que associava duas mulheres negras a gorilas. A empresa prometeu adotar soluções quanto à correção do viés, que só foi apresentada três anos depois, com a exclusão da base de dados do software dos termos de busca relacionado a animais e ainda quando da exclusão de imagem de primatas (OLIVEIRA, 2021).

O estudo *Face Recognation Vendor test* (FRVTV)[12] (GROTHER; NGAN.; HANAOKA, 2019), realizado por Grother, Ngan e Hanaoka, pesquisadores do *National Institute Stardards and Tecnologys* (NIST) dos EUA, em 2019, que tinha entre seus objetivos a análise dos perigos da segurança para o Estado, demonstrou na análise de 180 fornecedores que o sistema de RF errou de 10 a 100 vezes mais quando se tratava do reconhecimento de negros, indígenas ou asiáticos (SILVA, T., 2020).

Um marco no que concerne a divulgação e reconhecimento da existência de algoritmos enviesados que repercutiram na forma da difusão do racismo algoritmo e discriminação de gênero, sem dúvidas, foi a pesquisa Gender Shades de Buolamwini e Gebru (2018), do *Massachusetts Institute of Technology* (MIT).

Buolamwini e Gebru (2018) concluíram que as ferramentas de RF da Microsoft, IBM, Amazon, Face++ e Google apresentavam vieses raciais e de gênero, com uma taxa de erro maior no RF de pessoas negras, disparidade interseccional – ainda mais se comparados a mulheres negras, chegando a um percentual de 35% de vieses de treinamento. Nesse contexto, houve o desenvolvimento do PPB em que restou, demonstrado por Buolamwini e Gebru (2018), a possibilidade de diminuir os vieses racionais com uma base de dados mais diversa.

[12] O programa *Face Recognation Vendor test* (FRVTV), Part 3, foi desenvolvido pelo *National Institute Stardards and Tecnologys* (NIST) dos EUA.

A pesquisa teve um impacto direto nas grandes empresas de tecnologia, inclusive, em 2020, dentro do contexto da repercussão dos protestos mundiais pela morte de Jorge Floyd pela polícia de Mineápolis, EUA, no movimento *Black Lives Matter.* A Amazon, Microsoft e IBM baniram essa tecnologia de RF e reconheceram publicamente o enviesamento algoritmo racial e de gênero e o potencial nocivo da tecnologia quanto à violação dos direitos humanos pela ausência de regulamentação legal específica sobre esse tipo de tecnologia e falta de transparência de sua utilização, que poderia levar a uma vigilância ostensiva em massa pelo Estado.

Segundo Silva (2022), ao escrever sobre a **necropolítica algoritma**, a convergência do medo do espaço público com a crença de que a solução para a insegurança são mais polícias e mais tecnologia, esses fatores afetados pelo racismo, promovem o tecnochauvinismo, expressão de Meredith Broussard que significa:

> crença de que tecnologia é sempre a solução [...] usualmente é acompanhado por crenças próximas, como meritocracia, nos moldes de Ayn Rand; valores políticos tecnolibertários; celebração de liberdade de expressão, a ponto de negar que assédio on-line é um problema; a noção de que computadores são mais "objetivos" ou "sem vieses" porque eles destilam questões e respostas através de avaliação matemática. (SILVA, 2022, n.p.).

Tarcízio Silva (2019b) aponta quatro fatores que contribuem para o racismo algoritmo: o primeiro deles é a concentração de tecnologia em poucas empresas G.A.F.A. (Google, Apple, Facebook – atual Meta e Amazon), o que não seria positivo; o segundo, pouca diversidade de pessoas trabalhando nessas empresas; o terceiro, a falta de regulação social, na qual Tarcízio Silva (2019b) propõe a participação de representantes civis, casas legislativas e órgãos do governo e o quarto, de uma educação midiática, algoritma que teria como objetivo a difusão do conhecimento sobre a mídia e tecnologia e como funcionam, incluindo no ensino básico (SILVA, 2019b).

No Brasil, a realidade da cultura policial desfavorece os negros que são o alvo preferencial dos interrogatórios e revistas policiais, em razão de uma subcultura de rua de que os negros são mais propensos a ter um perfil de criminoso, o que não é realidade. Dessa maneira infelizmente o país ainda se vale do preconceituoso ditado popular de que "Branco correndo é atleta e Negro correndo é ladrão" (ALCADIPANI; PACHECO, 2020):

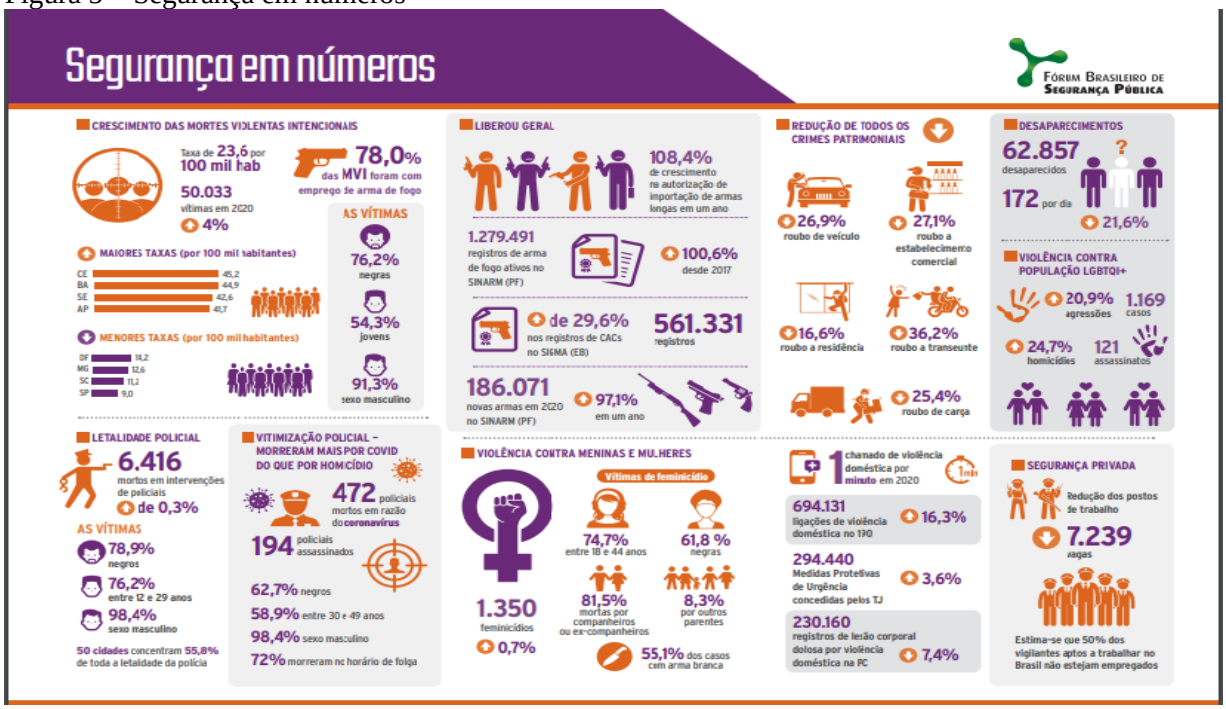
> No Brasil, o fazer da polícia se orienta muito mais pela subcultura de rua – conjunto de valores, conceitos e práticas passados dos policiais mais experientes aos iniciantes – do que por quaisquer protocolos. Segundo essa subcultura, o criminoso tem idade,

> cor, gírias, vestimenta, comportamentos e endereço pré-definidos. A alcunha de suspeito recai preferencialmente sobre corpos jovens, pobres, negros e periféricos, fazendo com que pessoas desse perfil sejam abordadas com uma frequência bem maior do que as de outros perfis. Em consequência, acabam sendo mais presas em flagrante. (ALCADIPANI; PACHECO, 2020, p. 1).

No que tange a aplicação do RF para fins de segurança pública, há preocupações ainda maiores por diversas associações de direitos humanos, visto que 90,5% das pessoas que foram presas no Brasil, com aplicação da TRF, são negros, consoante levantamento realizado pela Rede de Observatórios de Segurança no Relatório Retratos da Violência, cinco meses de monitoramento, análises e descobertas, em 2019 (RUBACK; ÁVILA; CANTERO, 2021, p. 5; OBSERVATÓRIO DE SEGURANÇA PÚBLICA, 2020).

O reflexo das abordagens da segurança pública aos negros também reflete nas mortes violentas provocadas por policiais e cujas vítimas foram predominantemente formadas de pessoas negras com o percentual de 78,9%, consoante dados do Anuário da Violência (2021), promovido pelo Fórum Brasileiro de Segurança Pública indicados na Figura 5:

Figura 5 – Segurança em números



Fonte: Alcadipani, Bueno e Lima (2021).

Ademais, um levantamento realizado pelo Colégio Nacional de Defensores Públicos Gerais (CONDEGE) constatou que, entre 2012 e 2020, 81% das prisões injustas, baseadas no reconhecimento fotográfico foram de pessoas negras, o que reflete o lado nefasto do racismo arraigado na sociedade e que se refletem em viés algoritmo que viola direitos humanos e priva inocentes da liberdade (RUBACK; ÁVILA; CANTERO, 2021). Uma realidade brasileira de

microagressões mais pervasivas, haja vista a suposição de uma pessoa racializada tenderia a ser mais perigosa e tendente a prática de crimes em razão de sua raça (SILVA, T., 2020a).

4.3.2 Sexismo Algoritmo

Além do racismo algoritmo, o RF pode apresentar também vieses por amostragem, por exemplo, através dos modelos de classificação de gênero, com aumento da falta de precisão para mulheres, fazendo com que a tecnologia possa adquirir um caráter machista/misógino por dolo ou culpa, em razão dos valores que trazem de seus desenvolvedores (OLIVEIRA, 2021).

Cumpre destaque que foi uma mulher quem criou o primeiro algoritmo do mundo. Em 1843, a matemática britânica Ada Augusta Bryon King, a Condessa de Lovelace, criou o primeiro código complexo de programação no mundo, em uma época em que mulheres sequer eram aceitas em universidade. Ada só foi reconhecida quando foi mencionada nos estudos de Turin, 1960, considerado um dos percussores da IA.

O Twitter, uma das maiores redes sociais do mundo, admitiu, em 2020, que os algoritmos que empregava em determinada aplicação de ferramenta de corte de imagem apresentava vieses racistas e sexistas e prometeu adotar medidas de correções. Safiya Noble (2018), ao analisar uma ferramenta de IA via RF do Google, concluiu pela existência de vieses racistas e sexistas no algoritmo avaliado na pesquisa, no que concerne ao fato de, ao se pesquisar por mulheres negras no Google, o algoritmo mostrar resultados de pesquisas com conteúdo pornográfico.

Nesse aspecto, Buolamwini e Gebru (2019), ao analisar o RF dos softwares da Amazon, IBM, Microsoft, Google e Face++, concluíram que, se comparado a identificação de mulheres negras, o índice de erros alcançaria 35%. Ainda, de forma geral foi constatado por uma pesquisa da Mckinsey, em 2010, que ao se pesquisar sobre cargos de liderança, por exemplo, CEO de empresas nos EUA, apenas 11% das imagens mostravam mulheres, sendo que o percentual era de 27% (FYLE, DOLA, *et al*, 2019), o que demonstrava o enviesamento de gênero.

Ainda, um outro ponto importante se trata da aplicação do RF pela segurança pública na identificação de rostos de pessoas transexuais, cisgêneros e não-binários, visto o enviesamento de avaliação e gênero algoritmo, também causada pela adoção de princípios higienistas em larga medida, na medida em que o RF se aplicaria em lugares estratégicos com os alvos determinados em razão da organização da ordem social por critérios políticos pré-estabelecidos (SILVA, 2021).

Segundo Viviane Medeiros, ativista e pesquisadora de gênero da Universidade Federal da Bahia (UFBA), há o receio de que o uso do RF termine por cercear direitos à população trans. Para a pesquisadora: "Achamos que essas tecnologias [RF e corporal] podem tornar as vidas trans como ilegítimas. Não é um estigma novo, mas é uma preocupação muito fundamental" (ALVES, 2021a, n.p.).

Uma pesquisa realizada pela Universidade de Colorado, EUA, realizada em 2019, sobre o RF dos transexuais, constatou que a precisão do RF, quando aplicado em mulheres, foi de 98,3%, sendo que, quando foi aplicado para transexuais, esse índice caiu para 87,3% (SILVA, 2021).

A pesquisa acima, realizada pela Universidade de Colorado, EUA, constatou que, quanto ao RF aplicado aos homens cisgêneros, o índice apontou uma assertividade de 97,6%, contudo, já para os homens trans, a precisão a média foi de 70,5%. E, quando se referem a pessoas não binárias, o resultante foi extremamente preocupante, visto que o índice de erro foi de 100% na pesquisa (SILVA, 2021), o que se torna preocupante a difusão do RF automatizado e a distância na segurança pública, em detrimento de tantos vieses que implicariam em possíveis violações aos direitos fundamentais da pessoa humana e que faz refletir quanto a necessidade de observação desses direitos para expansão da referida IA.

5 RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA SOB O OLHAR DOS DIREITOS FUNDAMENTAIS

Os direitos humanos são direitos básicos e universais, consagrados em âmbito internacional por normas e convenções, a exemplo da Declaração Universal de Direitos Humanos de 1948 que tem *status* universal, mas isso não significa que todos os direitos humanos são considerados como fundamentais dentro do contexto brasileiro.

Quando o trabalho se refere a direitos e garantias fundamentais da pessoa humana, envereda para o conceito dos direitos humanos que estão contidos na CF de 1988, classificados como cláusula pétrea, para efeito de proteção do Estado Democrático de Direito (BRASIL, 1988).

A CF enumera, em seu artigo 5º, caput, 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, X, 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).

Salienta-se, entretanto que, finalmente, em 10 de fevereiro de 2022, a proteção dos dados foi incluída na CF, como direito fundamental autônomo, através da aprovação do Projeto de Lei nº 17/2019, que resultou na aprovação na Emenda Constitucional (EC) nº 115, 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).

Segundo Peixoto (2012, p. 30), os direitos fundamentais podem ser classificados como uma categoria dogmática, pelo qual tem como finalidade a proteção da liberdade – *lato senso*, juridicamente prevista pelo Estado de Direito – Constitucional, podendo ser classificada como:

> 1) Analítica, preocupa-se com a construção sistemática e conceitual do direito positivo; 2) empírica, preocupa-se com as condições de eficácia a maneira como o legislador, a administração e os juízes os observam e aplicam nos contextos práticos; e 3) normativa, que pressupõe a fundamentação racional e jurídico-normativa dos juízos de valor, como, por exemplo, no processo de interpretação e aplicação. (PEIXOTO, 2012, p. 30).

Ao considerar as tecnologias de IA de RF na segurança pública, a justificativa dos gestores públicos é justamente o cumprimento do direito fundamental de segurança previsto na

CF. Para Lunardo e Silva (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, como: sistemas de vigilância, leis penais mais severas, controle de imigração etc.”.

Ainda, segundo os autores supramencionados, as ações acima “polarizam as duas reivindicações da sociedade, que são a garantia dos direitos individuais e a emergência do direito à segurança” (JOÃO; LUNARDO; SILVA, 2016, p. 27) e refletem na adoção de políticas públicas de segurança, como o RF por IA, que urge ser visto sob a ótica da liberdade, privacidade e proteção de dados pessoais.

5.1 LIBERDADE

A liberdade é considerada um direito fundamental e está previsto na CF de 1988 em seu artigo 5º, incisos IV, VI, XVI e XVII, no mesmo patamar de proteção da segurança e da privacidade:

> Art. 5º [...] IV - é livre a manifestação do pensamento, sendo vedado o anonimato; VI - é inviolável a liberdade de consciência e de crença, sendo assegurado o livre exercício dos cultos religiosos e garantida, na forma da lei, a proteção aos locais de culto e a suas liturgias; XVI - todos podem reunir-se pacificamente, sem armas, em locais abertos ao público, independentemente de autorização, desde que não frustrem outra reunião anteriormente convocada para o mesmo local, sendo apenas exigido prévio aviso à autoridade competente; XVII - é plena a liberdade de associação para fins lícitos, vedada a de caráter paramilitar.

Para Silva (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).

Uma aplicação deveras importante da TRF, quanto à questão da vigilância ostensiva provocada em razão da etnia, aconteceu, na China, com a minoria mulçumana Uighurs. Em 2018, a empresa Chinesa Huawei[13] desenvolveu uma *startup* denominada de Megvii, na qual o objetivo era o RF e indicar a estimativa de idade, sexo e etnia das pessoas. Esse software foi aplicado na etnia mulçumana chinesa Uighur e a cada rosto reconhecido emitia um alarme para a Huawei, realizando uma vigilância ostensiva, sem uma finalidade específica e sem transparência na utilização, violando, claramente o direito de liberdade dessas pessoas.

As pessoas que resistem ao sistema, por outro lado, podem sofre o efeito *chilling effect* – que é aquele em que o exercício da liberdade pode implicar em 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).

Silva, P. (2020, n.p.) conclui que 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".

No que tange a 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, 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, livre iniciativa, livre concorrência e defesa do consumidor, bem como demais princípios dispostos no MCI, a exemplo do respeito aos direitos humanos. Assim, o "Marco Civil fortalece uma visão antropocêntrica da AI – 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, previsto no artigo 3º, inciso VIII, do MCI (BRASIL, 2014a), permitir o desenvolvimento de aplicações na rede, a 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 – artigo 3º, incisos II, II, VI, VIII (DRUMMOND; CARNEIRO, 2022).

[13] Empresa que fornece a tecnologia de RF para o Estado da Bahia aplicar na Segurança Pública.

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

5.2 PRIVACIDADE

Para entender o contexto sobre o direito à privacidade, é importante fazer uma breve exposição histórica sobre o direito à intimidade, que está incluído no rol dos direitos da personalidade e tem por objetivo resguardar a dignidade humana, visto que a sua evolução impactou na construção do direito à privacidade.

O direito à intimidade está previsto em diversos documentos internacionais, a exemplo da Declaração dos Direitos do Homem e do Cidadão, de 1789, no artigo 12 da Declaração Universal dos Direitos do Homem, de 1948, no artigo 8º da Convenção Europeia dos Direitos do Homem de 1950. A CF de 1967 e a CF de 1988 em seu artigo 5º, inciso X, positivam a proteção da intimidade e acrescentaram a inviolabilidade da vida privada.

Em 1890, dois advogados de Havard, Samuel Warren e Loui Brandeis, escreveram um artigo chamado de *The Right to Privacy*, abordando pela primeira vez a menção a um direito à privacidade. “Os autores apresentam as características desse novo direito, suas funções e seus limites, distanciando-o da matriz proprietária utilizada como base para proteção de aspectos da vida privada até então, e aproximando-o da intenção de tutela da personalidade humana”, evoluindo para “o direito de estar só” (CANCELIER, 2017, p. 217).

A doutrina alemã apresentou a definição de privacidade, segundo a Teoria das Esferas, em que esta faria uma intersecção entre a esfera privada, esfera íntima e esfera secreta. Assim, na primeira, os fatos interpessoais, apesar de serem privados, poderiam ser divulgados; a segunda se relacionaria ao sigilo domiciliar e profissional, que seria mais restrito e limitado a divulgação, e a terceira se relacionaria a fatos ou atos que a pessoa não gostaria que fossem divulgados sem autorização (HIRATA, 2017).

Já a Teoria dos Círculos Concêntricos, criada na Alemanha na década de 1950, com base nas ideias de Heinrich Hubmann e Heinrich Henkel, apresenta a privacidade como finalidade de diferenciar o caráter público do privado, separando intimidade e segredo. O primeiro círculo seria o *privatsphare* – direito à privacidade em sentido estrito, o círculo do

meio é o *vertrauenssphare* – direito à intimidade e o círculo central corresponde à *geheimphare* ou *vertraulichkeitssphare* – direito ao segredo (COSTA JR., 1995).

O direito à privacidade está previsto no artigo 5º, inciso X, da CF (BRASIL, 1988) como "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" e no artigo 21 do Código Civil (BRASIL, 2002), sendo considerado 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 lei, por razões importantes e legítimas de interesse público" (ARANHA; TEIXEIRA, 2020).

O MCI previu o direito à privacidade no ambiente digital como princípio em seu artigo 3º, inciso III, bem como também no artigo 8º, inciso II, 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 no que tange ao crescimento das informações e ainda 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" (SOLOVE, 2011b; OLIVEIRA, 2021, p. 99).

Segundo Solove (2011b, p. 1), muitas vezes as solicitações de informações pessoais pelos governos não deixam as pessoas preocupadas pelo argumento de que "elas não teriam nada a esconder", o que permearia discussões sobre uma preocupação mínima com a privacidade e em um embate com a segurança, a vitória da segurança já estaria predestinada:

> When the government gathers or analyzes personal information, many people say they're not worried. "I've got nothing to hide," they declare. "Only if you're doing something wrong should you worry, and then you don't deserve to keep it private." The nothing-to-hide argument pervades discussions about privacy. The datasecurity expert Bruce Schneier calls it the "most common retort against privacy advocates [...] its most compelling form, it is an argument that the privacy interest is generally minimal, thus making the contest with security concerns a foreordained victory for security. (SOLOVE, 2011b, p. 1, grifos do autor).

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 e acesso das informações que podem estar concentradas no Estado, países ricos e empresas de tecnologias também são desafios para a Sociedade da Informação no que tange à democratização de acesso as tecnologias da informação comunicação e, consequente, o poder de controle (WERTHEIN, 2000).

Solove (2011) faz uma crítica a esse argumento do **nada a esconder**, que inclusive é utilizado como *slogan* de algumas políticas públicas de RF na segurança pública, a exemplo da polícia de Londres que utiliza **se você não tem nada a esconder, não tem nada a temer** (SOLOVE, 2011b), na medida em que dá a entender que a privacidade é algo ruim, quando se trata de um direito humano fundamental.

A massiva coleta de dados pessoais gera danos e apresenta um 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 as 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. "*To what extent should government officials have such a significant power over citizens?*", questiona Solove (2011a, p. 7), concluindo que o problema da utilização dos dados pessoais não é o que as pessoas tem a esconder, mas sobre poder, estrutura e governo.

Nesse sentido, o conceito de privacidade deve ser ampliado, assim os problemas não podem ficar restritos a " 'recolhimento' e 'divulgação", entre homem e prisioneiro de seus segredos e o homem que não tem nada a esconder; entre a 'casa e a fortaleza', que glorifica a privacidade e favorece o egocentrismo, e a 'casa-vitrine', que privilegia as trocas sociais" (RODOTÁ, 2008, p. 25, grifos do autor).

Diante do exposto, importante mencionar que, mesmo em uma sociedade da informação e vigilância que valoriza a superexposição, não querer se expor não deve ser algo condenável e a privacidade não deve ser um lugar de encarceramento (BAUMAN, 2014).

A evolução do conceito de privacidade – " 'do direito de estar só' até sobre o direito de controle sobre as informações pessoais e de construção de uma esfera privada" (OLIVEIRA,

2021, p. 101) – fez emergir um novo conceito de privacidade: a privacidade informacional ou a autodeterminação informacional (ARANHA; TEIXEIRA, 2021), ou seja, "a privacidade se consubstancia no 'direito do indivíduo de escolher aquilo que está disposto a revelar aos outros'". A privacidade evoluiu para "pessoa-informação-sigilo" para "pessoa-informação-circulação-controle" (RODOTÁ, 2008, p. 74 e 93).

O excesso de vigilância e controle pode ser nocivo à democracia, porque pode afetar negativamente a liberdade, a criatividade e o autodesenvolvimento (SOLOVE, 2008; OLIVERA, 2021). Nesse aspecto, a vigilância operada pelos sistemas de RF se torna uma forma muito ampla de poder investigatório, visto que registra o corpo, comportamentos, ações, interações sociais (OLIVEIRA, 2021; SOLOVE, 2008).

Para Rodotá (2004, p. 93), os programas de IA mais modernos se utilizam do controle ostensivo das grandes corporações nos quais analisam as expressões faciais, procurando descobrir os estados da alma, a esfera mais íntima das pessoas.

Os danos da vigilância via RF à privacidade se tornam mais contundentes, visto que na vigilância tradicional, em uma atividade investigativa, normalmente se investigam uma vez, já na vigilância por TRF se tornam permanente (OLIVEIRA, 2021).

As consequências desse controle ostensivo com a utilização biométrica das pessoas analisadas por *Big data* e *Big analytics* podem resultar "em uma sociedade na qual um indivíduo seja tratado como suspeito devido a uma sequência de encontros aleatórios ou inocentes, mas que foram julgados suspeitos por um sistema regulatório orientado por dados" (OLIVEIRA, 2021, p. 97), e o impacto seria da mudança do *status* social de "cidadãos livres" para "prisioneiros" (OLIVEIRA, 2021).

Para Maria Cecília Gomes, advogada e líder de projetos de proteção de dados da Fundação Getúlio Vargas (FGV), a análise das imagens coletadas, via RF, através do cruzamento de dados via base do poder público, deve obedecer a parâmetros, tais como transparência no cruzamento das imagens coletadas, divulgação da finalidade da coleta e proteção de dados pessoais dos titulares afetados pela política pública (ALVES, S., 2021a).

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. Pela relevância do tema, a proteção dos dados pessoais será explicitada no tópico específico, a seguir.

5.3 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, 2019). A proteção de dados se fundamenta na preservação da individualidade, liberdade e democracia (OLIVEIRA, 2021, p. 115).

Como já foi anteriormente exposto, a proteção dos dados pessoais foi recentemente incluída como um direito fundamental, na CF de 1988, com a inclusão da EC nº 115/2022 que incluiu o inciso LXXIX ao artigo 5º, e previu que "é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais" (BRASIL, 2022c). Ademais, a EC nº 115/2022 também alterou o artigo 22, inciso XXX da CF de 1988 para dispor a competência privativa da União para legislar sobre o tema. Essa inclusão foi um importante avanço na defesa do ser humano, como titular de dados pessoais.

Segundo a Ministra Rosa Weber do STF, no julgamento da Ação Direta de Inconstitucionalidade (ADIN) nº 6387/2020 da Medida Provisória (MP) nº 954/2020, "a proteção de dados pessoais e autodeterminação informativa são direitos fundamentais autônomos extraídos da garantia da inviolabilidade da intimidade e da vida privada e, consectariamente, do princípio da dignidade da pessoa humana" (BRASIL, 2020). Esse julgamento foi histórico, porque a proteção de dados pessoais foi considerada pela mais alta corte do judiciário brasileiro como um direito fundamental mesmo antes da previsão desse no rol constitucional.

Os dados pessoais são "informações relacionadas a pessoa natural identificada ou identificável". 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 ainda mais proteção, em razão de sua natureza, conforme o artigo 5º da LGPD.

A coleta dos dados pessoais pode ocorrer de duas formas: ou mediante interrogação ou vigilância (SOLOVE, 2011b). O primeiro, por exemplo, pode ser as respostas a um censo demográfico, o segundo pode significar uma forma de controle social (RODOTÁ, 2011).

No que se refere à interrogação, destaca-se o caso do censo de 1983, na Alemanha, que deu origem ao direito de autodeterminação informativa. Foi declarada inconstitucional pelo

Tribunal Constitucional da Alemanha Ocidental uma lei que criava um censo estatístico para a coleta de dados pessoais dos cidadãos para fins de políticas públicas em que cada cidadão deveria responder 160 perguntas que seriam tratadas de forma automatizada pelo governo (ARANHA; FERREIRA, 2020).

Segundo Aranha e Ferreira (2020, p. 2), destacam-se alguns motivos da declaração da inconstitucionalidade da lei do censo alemã e que ocasionou a importância da autodeterminação informativa dos dados pessoais. Dessa maneira, a primeira dimensão seria a da necessidade de transparência e a finalidade da utilização de seus dados e a segunda se trata do controle das pessoas de seus próprios dados pessoais:

> a) diversidade de finalidades, que impede que o cidadão conheça ou use o efetivo que seria feito com suas informações; b) desmistificação da noção de que o tratamento de certos tipos de dados pessoais seriamente irrelevante para a privacidade; c) o estágio de desenvolvimento de tecnologia usado no processamento de informações levantadas com o fator era um fator determinante, visto que a gravação de vídeos formados sobre dados dos critérios de uso ilimitado e provável pode causar danos aos indivíduos. (ARANHA; FERREIRA, 2020, p. 2).

Dessa maneira, "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" (ARANHA; FERREIRA, 2020, p. 2) e que tem extrema relevância quando se tratam de dados de IA pelo RF para fins de segurança pública.

Em 1995, foi aprovada a Diretiva 95/46 do Conselho da UE que estabeleceu, em seu artigo 1º, obrigações relativas ao tratamento de dados pessoais, de forma que houvesse um equilíbrio entre à vida privada e o desenvolvimento econômico. Torna-se importante essa regulação visto o alcance dessa diretiva a todos os países da UE.

Em seu artigo 2º, trouxe o conceito de dados pessoais e foi até mais explicativo do que o previsto na legislação brasileira de proteção de dados, visto que os dados pessoais se referiam até mesmo quando faz referência a um número de identificação ou a um ou mais elementos específicos da identidade física, fisiológica, psíquica, econômica, cultural ou social das pessoas.

Ainda, quanto a evolução legislativa da proteção de dados pessoais, a Carta dos Direitos Fundamentais da UE de 2000 se tornou um documento muito importante, visto que trouxe, no seu artigo 8º, a previsão da necessidade de consentimento ou de alguma base legal, para a utilização dos dados pessoais, além de prever o direito de correção e retificação de dados, além da criação de uma autoridade independente para fiscalização da utilização dos dados.

No Brasil, a LAI, Lei nº 12.527/2011 (BRASIL, 2011b), trouxe, em seu artigo 4º, o conceito de dados pessoais como "informação relacionada a pessoa natural identificada ou identificável". O MCI, Lei nº 12.964/2014 (BRASIL, 2014a) previu o direito à proteção de dados pessoais no ambiente digital ao estabelecer, em seu artigo 8º, inciso III, um princípio da disciplina do uso da internet no Brasil. Uma lei importante, mas limitada aos meios digitais.

Em 2016 foi aprovado na Europa o *General Data Protection Regulation* (GDPR), Regulamento nº 679/2016. Sem dúvida um dos documentos mais importantes na evolução do direito à proteção de dados pessoais, visto que dispôs que a proteção das pessoas naturais, em relação ao processamento de dados, é um direito fundamental, que deve servir ao ser humano, previu princípios que regem a utilização dos dados pessoais, tais como princípios da finalidade, necessidade, transparência, segurança da informação e não-discriminação e que foram replicados na legislação de proteção de dados brasileira.

De bastante relevância também é a Diretiva nº 680/2016 da UE que regulou o tratamento de dados pessoais para fins de segurança pública e persecução penal, quando, destacando-se a inclusão da necessidade de realização dos registros de atividade de tratamento, da inclusão da segurança e o sigilo dos dados e das disposições quanto à regulação da transferência internacional de dados.

Em 2018, foi aprovada, no Brasil, a LGPD, Lei nº 13.709/2018, mas que só entrou em vigor em totalidade no dia 18 de setembro de 2020. Uma lei extremamente importante para o país e de grande impacto na sociedade brasileira, visto a previsão de direitos do titular dos dados e obrigações da administração pública e empresas privadas quanto à proteção dos dados pessoais em suas atividades; e, ainda, com a obrigação das empresas desenvolverem um programa de privacidade e proteção de dados, de boa governança, criação do cargo de encarregado de proteção de dados, criação da Autoridade Nacional de Proteção de Dados (ANPD) e aplicações de sanções por descumprimento da lei.

O artigo 5º da LGPD (BRASIL, 2018b) subdivide os dados pessoais em sensíveis e anonimizados, sendo que, por definição legal, o "dado pessoal sensível é um dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" e que merecem ainda mais proteção pela administração pública e entidades privadas.

É importante ressalvar que, a princípio, em simples leitura da LGPD, essa lei não seria aplicável ao tratamento de dados exclusivos para segurança pública, defesa nacional, segurança do Estado e repressão de infrações penais – artigo 4º, inciso III, alíneas a), b) e c), 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 as questões principiológicas (BLUM; LOPEZ, 2020, p. 173) e que será melhor detalhado no próximo tópico, uma vez que essa lei tem uma importância ímpar no ordenamento jurídico brasileiro.

A coleta de pequenas informações de cada pessoa leva ao final a uma grande gama de informações concentradas no governo ou nas empresas de tecnologia – **pessoa digital**. Fato é que muitas dessas informações as pessoas não queriam dar publicidade ou pelo menos o titular dos dados deveria ter a escolha de compartilhar as informações ou não (SOLOVE, 2011a).

Especificamente, no caso da IA, em razão do baixo índice de invasão na coleta de dados biométricos e a facilidade na captação das imagens no RF, pode incentivar utilização excessivas da tecnologia (RODOTÁ, 2004, p. 100), ademais pode criar uma assimetria de poder entre as pessoas e as empresas e governos que detém os dados, causando incertezas e vulnerabilidades quanto ao seu uso no futuro (OLIVEIRA, 2021).

A proteção dos dados pessoais sensíveis é algo tão importante que, segundo a Agência Brasileira de Inteligência, a proteção vai além dos dados, abrange "a proteção física dos locais onde são produzidos, armazenados ou tratados os dados; a proteção das pessoas que gerenciam o local ou que vão manusear os dados e a proteção dos sistemas de informação" (AGÊNCIA BRASILEIRA DE INTELIGÊNCIA, 2016 *apud* GONÇALVES; MACHADO; VARELLA, 2018, p. 525).

Assim, é imprescindível que a administração pública também haja com precaução (BIONI, 2018) quando da contratação e utilização dessas tecnologias, a exemplo do RF, que podem ser mais invasivas aos direitos individuais.

Dessa maneira, "a proteção dos dados pessoais se transforma em um elemento essencial à liberdade individual na sociedade da vigilância" (OLIVEIRA, 2021, p. 123). Destarte, a regulamentação do RF automatizado, uma vez que pode ocasionar no controle de massas para fins políticos, econômicos e ideológicos e, por consequência, impactar nos direitos fundamentais da liberdade, privacidade e proteção de dados pessoais, se torna uma necessidade emergente a regulamentação dessa política pública, com o objetivo de conceder transparência em sua utilização na segurança pública.

6 (IN)EXISTÊNCIA DE REGULAÇÃO LEGAL ESPECÍFICA QUANTO À INTELIGÊNCIA ARTIFICIAL DE RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA

A aplicação do RF automatizado, via IA, como política pública de segurança já é uma realidade no mundo e no Brasil, o que se mostra de extrema importância investigar, se sob o aspecto legal regulatório, se há legislação que embase sua utilização como política de segurança pública.

O trabalho, dessa forma, a partir de agora se debruçará quanto a existência de normas legais regulatórias sobre o RF, especialmente no Reino Unido, países que integram a UE e EUA, abordando em seguida as tratativas legais sobre o tema no Brasil.

6.1 MUNDO

O Reino Unido, como já foi anteriormente mencionado quanto a exemplos de países que utilizam a TRF pelas polícias, se torna importante por ter sido um dos pioneiros no mundo a usar o videomonitoramento, desde 1953, e já ter chegado a marca de mais de seis milhões de câmeras de vigilância instaladas e boa aceitação dessa política pública entre as pessoas entrevistadas, o que só comprovaria o fundamento de Solove (2011a) de que no embate entre **segurança** e **privacidade** a tendência é de que a segurança prevaleça.

No mesmo sentido um estudo do *Instituto Lovelace*, realizado em 2019 no Reino Unido, constatou o apoio popular ao RF pelas polícias, no entanto, 55% das pessoas acreditaram que o governo deveria impor limites ao uso da TRF.

No Reino Unido não há legislação específica para tratar sobre a aplicação da TRF em locais públicos, mas há documentos de recomendação estratégica e regulatória que apontam diretrizes jurídicas para a administração pública, ademais há um ecossistema de instituições governamentais que monitoram o aparato estatal, a exemplo da *Biometrics Strategy: Better public services Maintaining public trust, Surveillance Camera Code of Practice, ICO Code of Practice for Surveillance Cameras e Metropolitan Police Legal Mandate for deploying Live Facial Recognition.*

A finalidade é a proteção da vida e da propriedade, manutenção de ameaças à segurança pública, prevenção e detecção de crimes, persecução criminal e garantia da segurança nacional. Há limites nos princípios da necessidade e proporcionalidade e antes de utilizar o TRF tem que avaliar se há maneiras menos invasivas. Deve haver protocolos de usos da tecnologia e no

âmbito da transparência a regulação do Reino Unido indica que as pessoas têm que ser avisadas do monitoramento em locais públicos e todas as pessoas gravadas tem direito de acesso as suas informações em até 40 dias, também há recomendação de realização de um Relatório de Impacto a Privacidade e Proteção de Dados (DPIA) (FRANCISCO; HUREL; RIELLI, 2020).

Nos EUA há legislação sobre o RF de forma genérica e dividida, marcada pelas legislações municipais. Por exemplo, em São Francisco há uma legislação: *San Francisco Ordinance* 190110: *Stop Secret Surveillance* e *Massachusetts Senate Bill* 1385/*House Bill* 1538, determinando o banimento da tecnologia por possível violação de direitos humanos, ao passo em que outros locais, como Flórida e Nova York, não há proibição. O Congresso Americano, em julho de 2021, realizou uma audiência pública para tratar a regulamentação do RF (GOIS, 2021).

O fato aconteceu após o *Government Accountability Office*, órgão que fiscaliza as contas do governo, requerer das agências federais americanas, como o *Federal Bureau of Investigation* (FBI), que sejam evitadas ações que desencadeiem em preconceitos e uso indevido em seus sistemas de RF (GOIS, 2021).

Quanto à tentativa de regulação da IA automatizada na segurança pública, a Agência dos Direitos Fundamentais da UE publicou o artigo *Facial recognation technology: fundamental rights considerations in the context of law enforcement* cujo objetivo foi de analisar as implicações da tecnologia frente aos direitos fundamentais da TRF para a segurança pública e controle das fronteiras, utilizando-se como base as disposições já presentes da GDPR, a exemplo de seu artigo 4º, item 14, com a descrição de biometria e artigo 9º, item 1, quanto à categoria da biometria como dados sensíveis (OLIVEIRA, 2021).

O artigo *Facial recognation technology: fundamental rights considerations in the context of law enforcement* vem a informar que qualquer utilização da TRF deve ser utilizada com análise de necessidade e proporcionalidade, assim, o fato de justificar a utilização da tecnologia com combate e prevenção de crimes, por si só não seria suficiente para a adoção invasiva dessa tecnologia; ainda que deve haver uma supervisão no uso da tecnologia para a proteção de dados como algo indispensável.

O Comitê Europeu para a Proteção de Dados (EDPB), que engloba todas as autoridades de proteção de dados da Europa, editou a Diretiva nº 3/2019 (EUROPA, 2019) sobre o tratamento de dados pessoais para o monitoramento em vídeo que foi implementada na UE em 2020, com base na regulação da GDPR. A diretiva apresenta como justificativa o fato de que, apesar das pessoas se sentirem confortáveis com a vigilância, poderá ser adotada em segundo plano para fins ilícitos e abusivos (OLIVEIRA, 2021).

Nesse sentido, a Diretiva nº 3/2019 (EUROPA, 2019) tratou sobre o âmbito de aplicação da tecnologia de videomonitoramento aos espaços públicos, com licitude de tratamento, de forma que os direitos do titular previstos na GDPR: autodeterminação informativa, duração do tratamento, correção e exclusão de seus dados e na Diretiva também sejam observados, a finalidade definida e específica na utilização dos dados e enquadramento em uma das bases legais previstas na GDPR, na qual não precisa ser necessariamente o consentimento.

Essa política pública só deve ser utilizada se outros meios legais menos invasivos não puderem ser utilizados. Deverão ainda ser aplicadas o princípio da minimização dos dados, ou seja, a coleta mínima dos dados sensíveis, de forma que os dados apresentem confiabilidade e integridade. Ainda, é importante destacar que a Diretiva nº 3/2019 (EUROPA, 2019) prevê a necessidade de realização de um relatório de impacto à proteção de dados, na forma definida pelo item 35 da GDPR, para reconhecer o alto risco dessa tecnologia aos direitos fundamentais.

Em 2021, a Comissão Europeia (EC) propôs uma regulação que limita o uso de IA com possíveis implicações globais dessas tecnologias, classificadas com base em risco. O RF foi classificado como de alto risco de violação aos direitos fundamentais da privacidade e proteção de dados, mas não foi proibido no projeto, que ainda está em discussão na Europa e apresentou bases dos documentos da EDPB de 2019.

Ocorre que o EDPB muda de entendimento e, em conjunto com a Autoridade Europeia para a Proteção de Dados (EDPS), em junho de 2021, emitiu uma recomendação, dessa vez, o banimento em espaços públicos através da tecnologia de IA, haja vista que o texto publicado em 2019 não foi suficiente para abranger todas as medidas necessárias à discussão do tema.

6.2 BRASIL

No Brasil não há legislação específica sobre a utilização do RF como política pública de segurança, todavia essas ações devem respeitar os princípios constitucionais e as leis de proteção de dados pessoais vigentes para evitar a violação de direitos fundamentais, apesar da crescente utilização dessa tecnologia em diversos Estados, a exemplo de São Paulo, Rio de Janeiro e Bahia.

Há a Lei de Inovação, Lei nº 10.973/2004, que tem por objetivo incentivar a inovação e a pesquisa científica e tecnológica visando a cumprir o objetivo da CF que é o de desenvolvimento do sistema produtivo, capacitação e autonomia tecnológica (art. 1º, caput), fornecendo bases para o desenvolvimento da IA ao prevê a aplicação da lei para criação, modelo

de utilidade e programa de computador que acarrete o surgimento de novo produto ou processo incremental (art. 2º, inciso II), contudo é uma lei bem generalista.

Sobre a questão regulatória da IA, ainda existe o Decreto nº 8.854/2019 (BRASIL, 2019c) que estabelece o Plano Nacional de IOT e que se fundamenta na **livre concorrência** e **livre circulação de dados**, bem como na **segurança da informação** e **proteção de dados pessoais** – art. 1º, mas também é uma norma genérica.

Apesar de ainda não ter uma regulação específica quanto ao RF na segurança pública, através da análise do ordenamento jurídico brasileiro, constata-se a possibilidade de aplicação de princípios, de forma geral, como balizadores de sua utilização e para a proteção dos direitos fundamentais.

6.2.1 Regulação por Princípios contidos na Lei Geral de Proteção de Dados Pessoais

Quando se trata de RF automatizado, por extração de biometria, para alguns autores, há a plena aplicabilidade da adoção de princípios previstos na LGPD na segurança pública, mas em razão da previsão do caput do artigo 4º da referida lei de que esta não se aplicaria a segurança pública a questão não é pacificada na doutrina.

Para Aras (2020, p. 156), "por possuir regime jurídico próprio, a autuação do poder público quanto à segurança pública, à defesa nacional, à segurança de Estado e às atividades de investigação e repressão de infrações penas são expressamente excluídas da incidência da LGPD". Aras (2020) continua a explanação informando que essa exclusão se justifica em razão do Princípio da Supremacia do Interesse Público.

Para Francisco, Hurel e Rielli (2020, p. 6), a operacionalização do RF automatizado por si já implica em tratamento de dado biométrico humano e, portanto, é resguardado pela LGPD:

> Para que qualquer sistema de reconhecimento facial funcione, é preciso que uma ou mais câmeras capturem a imagem de um rosto. Essa imagem será convertida em dados que correspondem a diversas características particulares da face de uma pessoa que, posteriormente, serão analisadas para o tratamento que se pretende. Tratam-se de dados resultantes de um tratamento específico de elementos físicos e fisiológicos – e eventualmente até mesmo comportamentais – singulares de uma pessoa, que permitem sua identificação. Isso significa que o reconhecimento facial funciona com base no tratamento de dados biométricos. Assim, qualquer emprego de sistemas de reconhecimento facial no Brasil deverá respeitar os princípios que utilizamos como critério de análise, tendo em vista sua previsão na Lei Geral de Proteção de Dados. (FRANCISCO; HUREL; RIELLI, 2020, p. 6).

Segundo o artigo 4º da LGPD, a lei não se aplica ao tratamento de dados pessoais para fins exclusivos de segurança pública, defesa nacional, segurança de estado ou atividades de repressão e investigação de infrações penais. Ocorre que, em seu parágrafo primeiro, a LGPD dispõe de que o tratamento de dados pessoais deverá ser previsto em lei específica, que deverá prever medidas proporcionais e estritamente necessárias ao interesse público, o devido processo legal e os princípios da proteção de dados.

O Poder Público, ainda que trate de dados sobre segurança pública deve obedecer aos princípios previstos na LGPD, conforme dispõe o parágrafo primeiro do artigo 4º da LGPD, quais sejam: 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 (BLUM; LOPEZ, 2020).

> **Finalidade**: a finalidade diz respeito aos propósitos que orientam o tratamento de dados pessoais. Estes devem ser sempre legítimos, específicos e explícitos, bem como não deve haver tratamento posterior que seja incompatível com essas finalidades.
> **Necessidade**: o princípio da necessidade relaciona-se diretamente à finalidade, apesar de não se confundir com a mesma. Aqui, procura-se garantir que o tratamento de dados pessoais seja restrito somente ao uso que se pretende, ou seja, ele deve ser limitado da melhor forma possível à necessidade do agente que coleta e trata os dados.
> **Transparência**: o princípio da transparência busca garantir que todos os titulares dos dados pessoais que serão tratados sejam informados a respeito desse tratamento. Essas informações precisam ser claras e de fácil acesso. Entende-se que, em certas situações, não será possível fornecer muitos detalhes, seja por razões de segredo industrial sobre a tecnologia empregada, ou em consequência da finalidade do tratamento, como por exemplo, nos casos em que os dados são usados para fins de segurança pública ou segurança nacional. Ainda assim, os titulares sempre terão o direito de acessar informações em linguagem acessível e simples sobre a realização do tratamento.
> **Segurança da informação**: o princípio da segurança tem como objetivo garantir que o tratamento de dados pessoais será feito de modo a atender critérios razoáveis de segurança e confidencialidade, evitando perda, destruição, alterações e vazamentos dos dados, bem como promovendo a utilização de ferramentas e políticas de proteção dos mesmos.
> **Não-discriminação**: este princípio determina que nenhum tratamento de dados pessoais pode ser realizado com fins discriminatórios, ou seja, não deve haver nenhuma forma de impacto ilegítimo nos titulares em consequência de características de gênero e orientação sexual, origem racial e social, posicionamento político, religião ou estado de saúde. (FRANCISCO; HUREL; RIELLI, 2020, p. 5-7, grifos nossos).

A utilização da anonimização dos dados pessoais pode trazer benefícios para a redução de riscos no que tange ao tratamento dos dados pela IA, visto que trará mais segurança ao titular dos dados e ainda permitirá um tratamento de uma maior base de dados para tratamento pelo desenvolvedor, visto que a LGPD não incide sobre esses dados. Ainda, a anonimização revela-se como incentivo a pesquisa (ITS, 2022).

Ainda, mister explicitar que o § 3º do artigo 4º da LGPD ainda dispõe expressamente da possibilidade da ANPD solicitar Relatórios de Impacto a Proteção de Dados Pessoais para o caso da segurança pública, o que é muito recomendável (FRANCISCO; HUREL; RIELLI, 2020). Apesar de não disposto expressamente na lei, a utilização pela segurança pública da privacidade como padrão – *Privacy by Desing* – decorre da interpretação finalística da LGPD (ITS, 2022).

O artigo 17 da LGPD (BRASIL, 2018b) vem a ratificar o direito da pessoa natural titular dos dados pessoais a liberdade, intimidade e de privacidade. Para Peck (2020, p. 99), é "possível relacionar essa garantia da pessoa natural a titularidade de seus dados à inviolabilidade de sua vida privada, pontuada por meio do artigo 5º, inciso X, da CF".

O artigo 18 da LGPD, também seria aplicável aos dados colhidos para fins de segurança pública, no que concerne ao direito dos titulares dos dados pessoais de ter a: I – confirmação do tratamento; II – acesso aos dados; III – correção de dados.

A LGPD é uma regulação de risco, por garantir direitos e prever princípios voltados para controladores e operadores de dados pessoais, como mecanismos de prestação de contas e sanções para calibrar o risco do tratamento de dados (FRANCISCO; HUREL; RIELLI, 2020). Dessa maneira, a LGPD deve ser aplicável à segurança pública.

6.2.2 Leis e Projetos de Lei no Brasil

Como já fora anteriormente informado, ainda não existe regulamentação específica sobre a utilização da IA de RF no Brasil, contudo existe uma lei do Distrito Federal, Lei nº 6.782/2020 (DISTRITO FEDERAL, 2020), e inúmeros projetos de lei federais e estaduais em trâmite, ressaltando-se, entretanto, que estes são genéricos e que não atenderiam a prevalência dos princípios de proteção de dados pessoais e privacidade.

Em abril de 2019, a Associação Brasileira de Inteligência (ABIN) realizou uma audiência pública e defendeu a regulação específica pelo Congresso para suprir as necessidades da segurança pública, tais como rastrear fugitivos, identificar agressores na multidão, localizar desaparecidos e acompanhar suspeitos de terrorismo. Segundo Felipe Soares, representante da ABIN, "a discussão legislativa deve buscar uma regulação que entenda que segurança e privacidade são conceitos complementares" (ABIN, 2019, n.p.).

No âmbito federal destacam-se os Projetos de Lei nº 9.736/2018, nº 9.414/2017 e nº 4612/2019. Os dois primeiros projetos apresentam em comum o fato de serem aplicados para setores específicos, respectivamente transporte público e estabelecimentos penais, o que por si

só já causaria limitação espacial, não preveem princípios a serem observados no RF e nem medidas de transparência ou prestação de contas ou de qualquer análise de risco (ITS, 2020, p. 14).

No que tange ao Projeto de Lei nº 4.612/2019 (BRASIL, 2019b), tem como objeto a regulamentação de tecnologias do RF e emocional, bem como outras tecnologias digitais voltadas a identificação de indivíduos à predição ou análise de comportamentos. Nesse projeto de lei há o reconhecimento do potencial perigoso quanto a vigilância em massa e a previsão de alguns princípios, além de obrigações específicas para desenvolvedores e utilizadores de RF e restrição de compartilhamento de dados, além do envolvimento da ANPD, mas ainda assim não especifica como seria o RF para fins de segurança pública.

No âmbito estadual, foi publicada a lei do Distrito Federal, Lei nº 6.782/2020 (DISTRITO FEDERAL, 2020), que regulamentou a utilização do RF em áreas públicas. Em breve síntese, a lei previu que houvesse prévio aviso as pessoas sobre o RF naquele espaço público, através de rastreio de movimentos físicos ou até mesmo de imagens estática em locais públicos, com a proibição a vigilância contínua.

Ainda, trouxe, a possibilidade de compartilhamento de dados com outras seguranças públicas e o armazenamento das imagens captadas durante cinco anos. Por fim, previu a revisão dos dados por um agente de segurança pública (G1-DISTRITO FEDERAL, 2020). Ocorre que, com a recente inclusão do inciso XXX ao artigo 22 da CF de 1988 que previu competência privativa da União para legislar sobre proteção de dados pessoais, a lei estadual poderá ser questionada na justiça quanto à sua validade jurídica.

O Laboratório de Políticas Públicas e Internet (LAPIN) elaborou uma nota técnica contendo algumas recomendações sobre a lei distrital acima, haja vista que regula uma matéria sensível, mas como lacunas referente a proteção de dados pessoais e a privacidade. Assim, a LAPIN (2021) recomendou dez pontos de adequação para a lei distrital:

> 1. Utilizar tecnologias de reconhecimento facial apenas em casos excepcionais, determinados, envolvendo investigações específicas e para procurar indivíduos já identificados, a fim de evitar a normalização e a vigilância em larga escala; 2. Definir os conceitos de espaços e equipamentos públicos e restringir o uso da tecnologia em áreas próximas a organizações religiosas, políticas, de tratamento de saúde ou similares, de forma a evitar ao máximo a captura de dados de natureza sensível; 3. Estabelecer protocolos de atuação e abordagem a serem seguidos pelos agentes em caso de alertas emitidos pelo sistema e que possam ser consultados facilmente pela população; 4. Definir critérios para utilização da tecnologia, tais como delimitar que seu uso seja feito exclusivamente para investigação de crimes de natureza grave, adotar mecanismos para minimizar o número de pessoas sujeitas a seu escrutínio e determinar o período máximo de aplicação, não ultrapassando 72h em nenhum caso; 5. Instituir protocolos de controle de acesso aos dados oriundos do sistema que restrinjam o tratamento de dados pessoais somente a pessoas que

> realmente necessitem acessar esses dados e registrem todos os acessos realizados; 6. Identificar as bases de dados utilizadas como fonte para o pareamento de imagens analisadas pelo sistema e informá-las à sociedade; 7. Estipular categorias de dados pessoais, definir tempos de armazenamentodistintos de acordo com a sua natureza, não ultrapassando 6 meses em qualquer hipótese, e estabelecer diretrizes para o compartilhamento de dados; 8. Adotar medidas de segurança e de proteção de dados, inclusive pseudonimização; 9. Instaurar procedimentos para o exercício de direitos do titular dos dados; 10. Elaborar Relatório de Impacto à Proteção de Dados antes da implementação da tecnologia e divulgar relatórios de transparência, de forma periódica, que contenham informações acerca do uso e dos resultados da tecnologia. (LAPIN, 2021).

Ainda, no âmbito estadual, foram identificados projetos de lei cujo objeto seria a regulamentação da tecnologia de RF automatizado, em que todos os projetos previram a finalidade de forma genérica, contudo não fazem uma análise de risco, não tratam os direitos dos titulares ou ainda relatórios de impacto e transparência (ITS, 2020, p. 14).

Segundo o ITS (2020), no Brasil há pelo menos 22 projetos de leis estaduais ou municipais que pretendem regulamentar o RF automatizado, inclusive para fins de segurança pública:

> Há ainda pelo menos três projetos dos 22 que preveem a instalação de sistemas de reconhecimento facial em áreas comuns, sem limitação espacial, com a finalidade genérica de identificação de criminosos e aumento da segurança para a população. Em Minas Gerais e Paraná, que fazem menção a tecnologias "trazidas da China", há previsão de que, em caso de eventual desvio de finalidade, "medidas adequadas" serão tomadas. Isso denota o reconhecimento de um risco no emprego da tecnologia, porém a resposta que a lei traz é genérica. 19 Amapá, Goiás, Minas Gerais, Paraná, Rio de Janeiro, São Paulo, Santa Catarina 20 PL 1893/19, PL 391/2019-MG, PL 148/2019-PR, PL 342/2019-RJ, PL 607/2019-RJ, PL 318/2019-RJ, PL 341/2019-RJ, PL 853/2019-RJ, PL 665/2019-RJ, PL 1101/2019-RJ, PL 1033/2019-RJ, PL 865/2019-SP 21 Goiás, Minas Gerais, Paraná, Rio de Janeiro e São Paulo. 22 PL 318/2019/RJ; PL 391/2019-MG, PL 148/2019-PR. (ITS, 2020, p. 14).

Ocorre que, com a inclusão do inciso XXX, ao artigo 22 da CF em 2022, a competência para regular sobre proteção de dados pessoais se tornou privativa da União.

O projeto de Lei nº 5.762/2019, também chamado de LGPD Penal, tem como objeto o tratamento de dados pessoais pelo setor público para fins de segurança pública e persecução criminal constante como proposta de regulamentação do artigo 4º, inciso III, da LGPD. A justificativa do projeto de lei é trazer

> balizas e parâmetros para operações de tratamento de dados pessoais no âmbito de atividades de segurança pública e de persecução criminal, equilibrando tanto a proteção do titular contra mau uso e abusos como acesso de autoridades a todo potencial de ferramentas e plataformas modernas para segurança pública e investigações. (BRASIL, 2019a, p. 1).

A exposição de motivos da LGPD Penal apresenta duas problemáticas que se referem a necessidade da aprovação do referido projeto de lei:

> O primeiro problema diz respeito à própria eficiência investigativa dos órgãos brasileiros, visto que a falta de adequação aos padrões internacionais de segurança quanto ao fluxo e ao tratamento de dados obsta a integração do Brasil com órgãos de inteligência e de investigação de caráter internacional (v.g., INTERPOL), obstando o próprio acesso a bancos de dados e a informações relevantes, e coloca o uso de aplicações tecnológicas em segurança pública e a adoção de técnicas modernas de investigação sob questionamento de sua validade jurídica. Em segundo lugar, há um enorme déficit de proteção dos cidadãos, visto que não há regulação geral sobre a licitude, a transparência ou a segurança do tratamento de dados em matéria penal, tampouco direitos estabelecidos ou requisitos para utilização de novas tecnologias que possibilitam um grau de vigilância e monitoramento impensável há alguns anos. Apesar do crescimento vertiginoso de novas técnicas de vigilância e de investigação, a ausência de regulamentação sobre o tema gera uma assimetria de poder muito grande entre os atores envolvidos (Estado e cidadão). Nesse contexto, o titular dos dados é deixado sem garantias normativas mínimas e mecanismos institucionais aplicáveis para resguardar seus direitos de personalidade, suas liberdades individuais e até a observância do devido processo legal. (BRASIL, 2019a, p. 1).

Em síntese, a proposta da LGPD Penal aborda, no seu artigo 9º,

> I - cumprimento de atribuição legal de autoridade competente, na persecução do interesse público, na forma de lei ou regulamento, observados princípios gerais de proteção, os direitos do titular; II - para execução de políticas públicas previstas em lei, na forma de regulamento e III - para a proteção da vida ou da incolumidade física do titular ou de terceiros. (BRASIL, 2019a).

Ocorre que o projeto vem recebendo críticas, em alguns de seus aspectos, por exemplo, a previsão do CNJ como a autoridade que emitirá recomendações e opiniões técnicas, e não prevê a ANPD, autoridade esta, competente para a fiscalização, orientação e aplicação de sanções, consoante artigo 4º, inciso III, §3º da LGPD (ITS, 2021).

O Projeto de Lei nº 5.762/2019 – LGPD Penal, em seu artigo 5º, inciso XXIII, define o que seria tecnologia de monitoramento como equipamentos, programas de computador ou sistema informático que possam ser usados para o tratamento de dados pessoais captados ou analisados, entre outros, em vídeo, imagem ou áudio e prevê a possibilidade de proibição de vigilância contínua em seus artigos 42 e 43, apesar de não estabelecer como se daria essa aferição de continuidade. Importante, observar que a lei do Distrito Federal previu 72 horas, contudo, a falta de previsão do projeto da LGPD penal abre uma brecha para abusos na vigilância (ITS, 2021).

Para Lemos e outros (2021), “o grande desafio da LGPD penal é estabelecer um equilíbrio entre a proteção de direitos individuais – como o direito de ir e vir, direito à proteção

de dados, privacidade e liberdade de expressão – e direitos coletivos como a segurança pública", que, segundo o ITS (2021), ainda não foi alcançado com o projeto de lei apresentado que abre brechas para a utilização indevida do RF na segurança pública.

Apesar das propostas legais acima ainda carecerem de uma maturidade quanto à previsão da possibilidade de utilização do RF automatizado na segurança pública, "somente com a regulação adequada das novas tecnologias de vigilância será possível impedir a consolidação da metáfora do homem de vidro, mitigando-se a eventual expropriação da liberdade, em todos os sentidos, que o progresso pode acarretar" (OLIVEIRA, 2021, p. 127).

A regulamentação das tecnologias de RF se torna importante pela ótica da uniformidade e segurança, por diminuir o problema da ausência de limites e diretrizes para aos programadores e empesas privadas que comercializam softwares. Na regulamentação, deve haver o destaque no que concerne a questões éticas e a transparência no tratamento dos dados das pessoas para persecução penal com privacidade e limites de compartilhamento e ainda com previsão de responsabilização por eventuais infrações, até para que as pessoas tenham como saber sobre a coleta de seus dados e possam se defender de possíveis abusos cometidos pelo Estado ou iniciativa privada (ARAUJO; CARDOSO; PAULA, 2021).

Para Silva, P., (2020, p. 4), as ferramentas de RF devem ser regulamentadas e não banidas, "por quatro forças regulatórias: normas sociais, jurídicas, econômicas e tecnológicas". O RF para a segurança pública, se controlado por disposições legais, poderia ser útil para a sociedade na promoção de políticas públicas.

Inclusive a resolução de 3 de maio de 2022 do Parlamento Europeu, ao tratar sobre os receios associados à IA, afirma que os riscos que atualmente se colocam relativamente às decisões tomadas com base na IA têm que ser tratados pelos legisladores, uma vez que já foi reconhecido de que efeitos nocivos relacionados à utilização desta, como a discriminação racial e sexual, já foram detectados em casos reais em que a IA foi utilizada sem salvaguarda de direitos (EUROPA, 2022).

Em março de 2022 foi instalada uma comissão de juristas com o objetivo de elaborar um projeto de regulação da IA no Brasil cujo objetivo foi tratar de contextos econômico-sociais e benefícios da IA, com destaque para questões relativas ao desenvolvimento sustentável e bem-estar, inovação, agricultura, indústria, serviços digitais, tecnologia da informação, robôs de assistência à saúde e também segurança pública (BRASIL, 2022b).

Essa comissão de juristas tem a relatoria de Laura Schertel e é presidida pelo Ministro do STJ Ricardo Villas Bôas Cuerva e ainda não foi finalizada. Segundo a relatora, na proposta de regulamentação da IA serão levados em consideração questões ligadas ao uso de dados

pessoais e sem o uso de dados pessoais, bem como a mineração de dados e com destaque para o princípio da precaução (BRASIL, 2022b).

Na quarta audiência pública realizada pela comissão de juristas, acima mencionada, se destacou o mencionado por Silva (2022, p. 10) no sentido de que a regulação da IA não só deve ser vista por uma perspectiva principiológica, mas sim que sejam utilizados mecanismos de *enforcement*. "E o compromisso, considerando todo o histórico, que temos já registrado de discriminação e racismo algoritmo, sobre a inclusão explícita de antirracismo e discriminação negativas interseccionais", nesse esteio, Silva, T. (2022) promoveu a defesa do banimento do reconhecimento automatizado para fins de segurança pública.

6.3 PROPOSTAS DE BANIMENTO DO RECONHECIMENTO FACIAL

A utilização da tecnologia de RF, seus vieses, inclusive raciais e de gênero, contribuem para o aumento do racismo algoritmo e do panoptismo digital, na medida em que políticas públicas de segurança pública, travestidas de objetivos de segurança e liberdade, são utilizadas para marginalizar as minorias, fazendo com o que o princípio da presunção da inocência e da privacidade e proteção de dados pessoais sejam ultrajados em razão da aplicação da vigilância ostensiva pelo Estado (SILVA, T. 2020a). "Será que estamos cada vez mais presos dentro de um aparelho estilo *Panoptican*? Vivemos Bentham na época dos Bits?" (DAWLER, 2001, p. 4, grifo do autor).

Como mencionado acima, o EDPB mudou de entendimento em junho de 2021 e, junto com a EDPS, recomendou o banimento em espaços públicos através da tecnologia de IA. A opinião recomendou que, entre as proibições, deve-se incluir "o reconhecimento automatizado de características humanas, como reconhecimento de rostos, formas de andar, impressões digitais, DNA, voz e outros sinais biométricos ou comportamentais, em qualquer contexto" (EDPB; EDPS, 2021, n.p.).

Segundo Andrea Jelinek, presidente da EDPB, e Wojciech Wiewiórowski, EDPS:

> A implantação da identificação biométrica remota em espaços acessíveis ao público significa o fim do anonimato nesses locais. Aplicações como o reconhecimento facial ao vivo interferem nos direitos e liberdades fundamentais de tal forma que podem pôr em causa a essência desses direitos e liberdades. Isso exige uma aplicação imediata da abordagem de precaução. Uma proibição geral do uso de reconhecimento facial em áreas acessíveis ao público é o ponto de partida necessário se quisermos preservar nossas liberdades e criar uma estrutura legal centrada no ser humano para a IA. O regulamento proposto também deve proibir qualquer tipo de uso de IA para pontuação social, pois é contra os valores fundamentais da UE e pode levar à discriminação. (EDPB, 2021, tradução nossa).

É importante mencionar a *Ordinance* nº 107-19, da cidade de São Francisco, Califórnia, EUA, visto que determina o banimento da tecnologia de RF para fins de vigilância. Essa legislação é muito simbólica porque a cidade de São Francisco fica no Vale do Silício, região conhecida mundialmente como o berço da tecnologia e onde se encontram as maiores empresas de inovação e tecnologia do mundo, como Apple, Google, Microsoft e Tesla.

A *Ordinance* nº 107-2019 reconhece que as tecnologias de vigilância representam uma ameaça aos direitos fundamentais da privacidade e que estas tecnologias serviram historicamente para perseguir minorias étnicas, com viés raciais, gênero, religião ou com ideologias políticas diferentes e ainda estabelece que o potencial perigo desse tipo de tecnologia violar os direitos fundamentais supera os possíveis benefícios. A cidade de São Francisco adotou o princípio da precaução.

O princípio da precaução é muito utilizado no direito ambiental, definido na Declaração do Rio 92 sobre Meio Ambiente e Desenvolvimento realizada em 1992 no Rio de Janeiro, e que afirma que uma abordagem precaucionaria deve ser aplicada pelo Estado, de acordo com suas capacidades para a proteção do meio ambiente (BIONI; LUCIANO, 2019).

O princípio da precaução pode ser invocado para avaliação de riscos, com potencial dano, sério ou irreversível e não deve ser invocado de forma indiscriminada, "nesse sentido, o princípio da precaução reconheceria as assimetrias de poder e de informação dos processos de avaliação regulatória e ajudaria a remodelar os diferentes conhecimentos dos diversos atores envolvidos e afetados por esses processos" (BIONI; LUCIANO, 2019, p. 7), fomentando a criação de pesquisas objetivando informações sobre riscos desconhecidos.

Quando dos protestos *Black Lives Matter*, após a morte de George Floyd, nos EUA, a repercussão mundial sobre o racismo policial na abordagem e investigação de negros gerou outra polêmica, que foi a aplicação do RF pela polícia americana para identificar pessoas que participaram dos protestos, em uma clara violação dos direitos de liberdade de associação e reunião (OLIVEIRA, 2021).

Ademais, a repercussão negativa da utilização desvirtuada da finalidade e a pressão popular fizeram com que medidas drásticas fossem tomadas pelas gigantes da tecnologia Amazon, Microsoft e IBM em 2020, quanto a banir nos EUA seus softwares de RF, com o reconhecimento oficial da possibilidade do uso nocivo das tecnologias.

Em razão do alto grau de sensibilidade dos dados biométricos "a capacidade de precisão dos sistemas e os potenciais benefícios setoriais não podem se sobrepor ao debate sobre direitos e proporcionalidades do uso", constituindo assim em um alto grau de monitoramento intrusivo,

na maioria das vezes, em que o titular dos dados não sabe nem que a coleta está sendo realizada (FRANCISCO; HUREL; RIELLI, 2020).

A IBM, em 09 de novembro de 2020, anunciou o banimento da tecnologia de RF da empresa, através de uma carta aberta endereçada ao presidente americano John Biden, em que reconhecia que não toleraria o uso da RF para vigilância em massa, perfis raciais, violações de direitos humanos ou qualquer finalidade que não observasse os valores da empresa e os princípios da confiança e transparência e requeria do governo americano uma regulamentação de precisão para ajudar na criação de barreiras éticas para o uso da tecnologia sem prejudicar as inovações tecnológicas.

No que tange a aplicação do RF para fins de segurança pública, há preocupações ainda maiores por diversas associações de direitos humanos, visto que 90,5% das pessoas que foram presas no Brasil, com aplicação da RF, são negros, consoante levantamento realizado pela Rede de Observatórios de Segurança, em 2019 (OBSERVATÓRIO DE SEGURANÇA PÚBLICA, 2019).

Para Silva, T. (2021), urge a necessidade de banimento da tecnologia de RF para fins de segurança pública e elege dez razões para o banimento. A primeira delas se refere à imprecisão das tecnologias e maior incidência de erros em pessoas racializadas e todos os vieses que apresentam para pessoas negras.

O segundo seria a seletividade penal como norma nas polícias e na justiça em que, segundo Silva, T. (2021) seria "construída desde o seu início como ferramentas de controle de populações vulneráveis e manutenção de relações de exploração e subjugação de classe, racialmente e patriarcalmente definidas", conclui ainda Silva, T. (2021) que em razão das polícias "errarem mais contra pessoas negras e pobres", não se poderia deixar de apoiar um posicionamento abolicionista da TRF na segurança pública, também por um posicionamento de não apoiar mais formas de promoção do encarceramento (SILVA, T., 2021).

O terceiro ponto seria de que tecnologias digitais vistas como **neutras** ou **objetivas** favorecem excessos policiais. Silva, T. (2021), utiliza o exemplo do RF em Londres, em que ficou comprovado que os policiais desrespeitavam o protocolo de abordagem das pessoas no RF.

A quarta razão se refere a menção a segredo de negócio ou inexplicabilidade algorítma para que as empresas de tecnologia não informem com transparência a operacionalização da TRF.

O quinto ponto se refere a pressuposição de aumento da vigilância nos espaços públicos como ubíquas e pervasivas favorecendo uma compreensão do espaço público como de vigilância continua e indiscriminada.

O sexto, seria a presunção de boa-fé das empresas de tecnologia, haja vista exemplos de manipulações de dados, escândalos de corrupção.

O sétimo seria relativo ao vazamento de milhares de dados pessoais por ataque de cibercriminosos, ou ainda por falhas de segurança as empresas de tecnologia e governos, que deve desencorajar o acúmulo massivos de dados, principalmente, os biométricos, haja vista a possibilidade de danos irreversíveis (SILVA, T., 2021).

A oitava razão do banimento da TRF seria a infraestrutura de violência que aumenta potencial violento de projetos autoritários. Nesse aspecto, Silva, T. (2021) chama a atenção para a utilização ostensiva em governos não democráticos, ou ainda em caso de guerra ou mudança institucional se tornar uma arma de potencial inédito de dano.

O nono ponto se trata da falta de imprecisão de reconhecimento de gênero, o que provoca maiores violações a seus direitos fundamentais.

E o décimo, diz respeito ao que o custo-benefício da coleta massiva de dados não justifica a coleta massiva de dados (SILVA, T., 2021).

Para Ferreira (2022), em sua palestra no 12º Fórum da Internet no Brasil, a premissa de pretensa isenção, neutralidade das ferramentas de tecnologia aplicadas à segurança pública, porque seriam baseadas em cálculos matemáticos sem erros não existe, uma vez que estes se baseiam em dados inseridos cuja compreensão é essencialmente **branconcêntrica**, na medida em que vieses na formulação da tecnologia tem impacto na precisão da tecnologia em corpos pretos e genderizados.

Ferreira (2022) ainda conclui que a segurança pública ao adotar o RF, “este se torna mais uma ferramenta aos dispositivos estatais, no sentido de Foucault, formas conjunturas de controle sobre corpos lidos como corpos indesejados, em uma ferramenta que afirma ser neutra mais não é”. Ferreira (2022) defende o banimento da tecnologia de RF na segurança pública, porque, segundo ela, seu uso viola o Princípio da Presunção de Inocência.

Na Itália, em 16 de abril de 2021, a Fiador, que corresponde a sua autoridade de proteção de dados pessoais, emitiu um parecer desfavorável ao sistema de RF *Sari Real Time*, utilizada pela polícia italiana. O sistema *Sari* realizaria um tratamento automatizado dos dados em larga escala, sem local definido e de forma universal, a autoridade italiana entendeu que o sistema *Sari* poderia violar direitos humanos fundamentais da privacidade e proteção de dados e ainda

contribuir para a vigilância em manifestações violando o direito de liberdade de associação e a presunção de inocência (LIMA, 2021).

Destaca-se que foi elaborada uma carta aberta por: *Access Now*, *Amnesty International*, *European Digital Rights* (EDRi), *Human Rights Watch*, *Internet Freedom Foundation* (IFF) e o Instituto Brasileiro de Defesa do Consumidor (IDEC), com adesão de mais 170 entidades e instituições de direitos humanos em que requereram o banimento da utilização do RF automatizado como política de segurança pública e que houve uma grande repercussão mundial desse documento.

A base da carta aberta de banimento acima mencionada se justifica em razão de que a vigilância em massa pode se dar através de uma vigilância discriminatória e direcionada, rastreando seres humanos e violando direitos à privacidade e à proteção de dados, o direito à liberdade de expressão, e os direitos à igualdade e à não-discriminação, o direito à liberdade de reunião e associação, com inibição de criminalização de protestos.

Na carta aberta foram citados locais em que foram identificados abusos na utilização da TRF, a exemplo de Myanmar, Dubai, EUA, Emirados Árabes, com a prisão de manifestantes, Argentina e Brasil, com erros do RF, ocasionando prisão de inocentes, e ainda China, Tailândia e Itália, com a vigilância de minorias étnicas e religiosas ou outras comunidades reprimidas. Para *Access Now*, *Amnesty International*, EDRi, *Human Rights Watch*, IFF e o IDEC, a TRF carece de p*rivacy by design* [privacidade desde a concepção] e ameaçam os direitos dos cidadãos; dessa maneira, regulações legais não poderiam eliminar todos os riscos aos direitos humanos de uma vigilância massiva e seus possíveis danos.

Recentemente, em 31 de maio de 2022, foi lançada a campanha *Tire o meu rosto da sua mira*, mobilização da sociedade civil pelo banimento total do uso das tecnologias digitais de RF na segurança pública, que reflete o pleito de entidades de defesa dos direitos humanos, pelo pedido de banimento da tecnologia, por reforçar o encarceramento, principalmente de pessoas racializadas e estigmatizadas (FÓRUM DA INTERNET DO BRASIL, 2022).

Ainda, o coletivo baiano Aqualtunelab também se manifestou favorável ao banimento da tecnologia, para fins de segurança pública, ao enviar sugestões para a comissão de juristas que está realizando estudos sobre a regulação legal da IA no Brasil, em razão dessa tecnologia ser considerada de alto risco aos direitos fundamentais. A proposição do Aqualtunelab é de que a tecnologia seja banida até que possa apresentar resultados que eliminem os riscos de discriminação racial e violação de direitos fundamentais (AQUALTUNELAB, 2022).

Não obstante a indefinição regulatória quanto ao videomonitoramento por RF automatizado, o Brasil, através de seus governantes, vem cada vez mais implementando essa

tecnologia como política de segurança pública, apresentando como justificativa a preservação da segurança e medidas de custo-benefício, com destaque para o Estado da Bahia, através dos projetos Vídeo Policiamento – Mais Inteligência na Segurança e Vídeo-Polícia Expansão da SSP-BA e PRODETUR-Salvador do Município de Salvador, como será demonstrado nosapontamentos metodológicos a seguir.

7 APONTAMENTOS METODOLÓGICOS

Para melhor compreensão de como foi desenvolvida a pesquisa, se torna de extrema importância traçar os caminhos metodológicos aplicados. Quanto à natureza, a tônica utilizada para o trabalho foi de pesquisa qualitativa. Segundo Silveira e Córdova (2009, p. 32), são características da pesquisa qualitativa: "objetivação do fenômeno; hierarquização das ações de descrever, compreender, explicar, precisão das relações entre o global e o local em determinado fenômeno".

Na pesquisa qualitativa, o pesquisador faz seu estudo utilizando as ciências humanas e subjetivas, dessa maneira é importante ressaltar que alguns fatores são importantes para a pesquisa, tais como a condição do ambiente e os dados culturais (OLIVEIRA, 2009).

A pesquisa trata de uma temática nova, interdisciplinar, ao conjugar aspectos jurídicos, técnicos e sociais, além disso, tem também como escopo principal responder a um problema baseado na análise de uma política pública: RF na segurança pública do Estado da Bahia, com apenas quatro anos de utilização até a presente data, e baseada em tratamento de tecnologias e informações pouco conhecidas pela sociedade. Assim, no caso em tela, as pesquisas qualitativas são mais adequadas porque concerne ao estudo de realidades pouco conhecidas (VIEIRA, 2009).

Para se alcançar os objetivos do estudo, anteriormente expostos quando da introdução, foi desenvolvida uma pesquisa exploratória. Para Gil (2002), essa pesquisa tem como objetivo principal o aprimoramento de ideias ou descobertas de intuições. Segundo Gil (2002), o planejamento de pesquisa pode ser flexível, de forma a considerar variados aspectos relativos ao fato estudado.

Nesse esteio, Gil (2002, p. 41) entende que na maioria das pesquisas exploratórias há o envolvimento de três fatores: levantamento bibliográfico, entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado, e análise de exemplos que **estimule compreensão**. Ademais, a pesquisa obedeceu a um método dedutivo, mediante descrição, exploração e discussões teóricas, método este que utiliza o silogismo, uma construção lógica em que parte de duas premissas e retira-se uma terceira, que decorre da análise lógica das duas primeiras (SILVA; MENEZES, 2005).

O levantamento bibliográfico para a pesquisa foi realizado, utilizando-se de referências teóricas publicadas em meio físico e digital, livros, teses, dissertações, artigos científicos e revistas científicas eletrônicas, coletados mediante a busca de palavras-chave sobre o tema: IA, RF, proteção de dados pessoais, privacidade e segurança pública.

À luz da perspectiva histórica e além da utilização de palavras-chave na pesquisa, o levantamento bibliográfico se concentrou na identificação de teorias e autores que tratavam sobre o tema. Para tanto, foram observados nos textos pesquisados quais eram os autores que constituíam as referências bibliográficas e a frequência como eram repetidos nos materiais de estudo para formação do referencial teórico deste trabalho, conforme indicado no Quadro 3:

Quadro 3 – Objetivos específicos, categoria de análise, contribuições/desafios, principais autores

continua

Objetivos específicos	**Categoria de análise**	**Contribuições/ Desafios**	**Principais autores**
1) descrever a evolução da sociedade e o impacto das TICs, de forma a perpassar pela Sociedade da Informação, Quarta Revolução Industrial até o desenvolvimento do Panoptismo Digital.	TICs.	Histórico, conceito, características, campo aplicação, evolução e contribuições.	Castells (1999, 2004); Schwab (2016); Peck (2019); Menezes (2022); Werthein (2000); Augusto (2019); Levy (1999, 2011); Vidal (2005); Lopes (2008); Zuboff (2018); Silva Neto, Bonacelli e Pacheco (2020); Han (2018); Siqueira e Lara (2020); Oliveira (2021); Vidal (2014); Pogrebinschi (2004); Foucault (1999, 2001, 2011); Koerner (2020), Rodotá (2008).
2) identificar planos e/ou projetos no Brasil realizados a partir de políticas públicas que aplicaram tecnologias de IA, particularmente as de RF;	TICs como Política de Segurança Pública, IA, RF.	Histórico, evolução, conceitos, características técnicas, apresentação de elementos gráficos e tabelas.	Santos, Lima e Souza (2020); Alcadipani (2021, 2022); Albardeiro (2020); Pagan (2021); Duarte (2022); Silva (2020); Norris e Armstrong (1999); Solove (2011); Nunes e outros (2016); Oliveira (2020); Bonamigo, Pedro e Melgaço (2016); Rosa (2011); Kaufman (2018), Magalhães e Vieira (2020); Siqueira e Lara (2020); Franqueira, Hartmann e Silva (2020); Hora (2021); Alves (2020).
3) analisar a utilização (contribuições e limites) da tecnologia de RF utilizado pelo Estado, sob a ótica dos direitos fundamentais da liberdade, privacidade e proteção dos dados pessoais.	RF Automatizado como Política de Segurança Pública.	Apresentação de limitações técnicas e vieses algorítmicos, características, aplicação de conceitos, análise de pesquisas.	Oliveira (2021); Rodotá (2008); Solove (2011); Vidal (2014); Ruback, Ávila e Canteiro (2021); Russel e Noving (2013); Silva (2020); Hong (2020); Goulart e Timm (2020); Mckinsey (2019); Buolmwini e Gebru (2018; Norris e Armstrong (1999); Pacheco (2020); Observatório de Segurança Pública (2020).
3) analisar a utilização (contribuições e limites) da tecnologia de RF utilizado pelo Estado, sob a ótica dos direitos fundamentais da	Direitos Fundamentais da Liberdade, Privacidade e Proteção de Dados Pessoais.	Conceitos, instrumentos legais, legislação comparada.	Peixoto (2012); ITS (2022); Negri, Oliveira e Costa (2020); Solove (2011); Cancelier (2017); Doneda (2006); Oliveira (2021); Rodotá (2008); Bauman (2014);

Objetivos específicos	Categoria de análise	Contribuições/ Desafios	Principais autores
liberdade, privacidade e proteção dos dados pessoais.			Aranha e Teixeira (2021); Bioni (2019).
4) investigar a existência de regulamentação legal para o uso da IA de RF na segurança pública no mundo e no Brasil.	(In)Existência de legislação específica sobre RF aplicada a segurança pública no mundo e no Brasil.	Pesquisa de instrumentos legais de regulação, princípios, projetos de lei, proposta de banimento da tecnologia.	Bioni (2019); Francisco, Hurel e Rielli (2020); Oliveira (2021); Blum e Lopes (2020); Drummond e Carneiro (2022); Lapin (2020); Araujo Cardoso e Paula (2021); Dawler (2001); Silva (2020); Silva (2020); Ruback, Ávila e Cantero (2021).
5) analisar os principais benefícios e riscos da implementação da política pública de utilização da tecnologia de IA, por RF, aplicada pela SSP-BA, visando apresentar, discutir e propor melhorias aos projetos Vídeo Policiamento – Mais Inteligência na Segurança, Vídeo-Polícia Expansão e PRODETUR Salvador.	Política pública de RF, via IA, aplicada nos projetos Vídeo Policiamento – Mais Inteligência na Segurança; Vídeo-Polícia Expansão e PRODETUR Salvador.	Histórico, evolução, benefícios e desafios, proposição de melhorias.	Freitas Filho (2018); Pires e outros (2021); Prescott e Mariano (2018); Salviano (2019); Falcão (2021); Muniz (2019); Andrade (2019); Palma, Pacheco (2020).

Fonte: Elaborado pela autora (2022).

É importante destacar que também foi adotada a técnica de análise documental de forma complementar. Para Oliveira (2021, p. 36), "a técnica da análise documental é extremamente importante para que deduções válidas sejam realizadas, a partir de documentos selecionados". Assim, na realização da avaliação preliminar documental e na análise dos dados obtidos na pesquisa, observou-se alguns aspectos: contexto histórico, autores, confiabilidade e credibilidade, interesses na escrita do tema, natureza do texto e conceitos-chaves (CELLARD, 2008), conforme anteriormente explicado.

Cellard (2008) e Godoy (1995) entendem ser um documento, muito além do que somente na forma escrita, a exemplo de jornais, revistas, obras literárias, relatórios; estatísticas e elementos iconográficos, mas também filmes, vídeos, imagem e fotografias, por exemplo.

Para Godoy (1995, p. 21-22,), "os documentos são considerados "primários" quando produzidos por pessoas que vivenciaram [...] o evento que está sendo estudado, ou "secundários", quando coletados por pessoas que não estavam presentes por ocasião da sua ocorrência". Dessa maneira, na pesquisa serão considerados para análise os documentos secundários.

Foram analisados os documentos secundários, em face dos materiais colhidos pela internet de leis, diretivas, regulamentos, projetos de lei, editais e termos de referência para

licitação, dissertações de mestrado e teses de doutorado digitais, sites institucionais dos governos, de associações e autoridades de proteção de dados no Brasil e no mundo e ainda documentários, palestras na plataforma YouTube, sites de jornais, revistas eletrônicas, portais de notícias e sites de busca – Google acadêmico – e Scielo.

No âmbito nacional foram objeto de estudo os direitos fundamentais da liberdade, privacidade e proteção de dados pessoais, previstos na CF em seu artigo 5º, respectivamente: incisos IV, VI, XVI e XVII, X e LXXIV.

A pesquisa continuou perpassando por mais dispositivos legais, a exemplo da Lei nº 12.527/2011, conhecida como LAI, que foi utilizada na pesquisa de forma conceitual, quanto as suas diretrizes de transparência na utilização das informações pela administração pública, bem como pela invocação desta perante a SSP-BA para requerer informações sobre o RF aplicado no Estado para fins de segurança pública e repressão criminal.

O MCI, Lei nº 12.965/2014, também teve um papel de destaque na pesquisa, haja vista ser um instrumento normativo em que contém, como princípios, em seu artigo 3º, incisos I e II, a privacidade e a proteção de dados pessoais para os titulares no uso da internet.

A pesquisa continua e adentra na LGPD, Lei nº 13.709/2018, principal legislação específica sobre a proteção dos dados pessoais no Brasil, um marco regulatório de proteção dos direitos dos titulares dos dados pessoais da utilização indevida pela iniciativa privada e administração pública.

A LGPD (BRASIL, 2018b) confere à administração pública uma base legal de coleta, tratamento, utilização e compartilhamento de dados pessoais para promoção de políticas públicas (artigo 7º, inciso III), mas impõe princípios e obrigações que devem ser seguidas para tal utilização, tais como a utilização para atendimento da finalidade pública e persecução do interesse público (artigo 23).

Ainda, foram relevantes para a pesquisa, o estudo do Projeto de Lei nº 5.762/2019 – conhecido como a LGPD Penal, por ser dedicado a tratar especificamente sobre a proteção de dados pessoais para fins penais, repressão de crimes e segurança pública. No âmbito federal se destacam os Projetos de Lei nº 9.736/2018, nº 9.414/2017 e nº 4612/2019.

Por fim, no aspecto legal brasileiro, foi estudado o Projeto de Lei nº 21/2020 que é considerado o marco regulatório da IA no Brasil e que já teve aprovação da Câmara dos Deputados, mas atualmente se encontra em trâmite no Senado Federal com pedido de tramitação em caráter de urgência e outros projetos de lei em caráter estadual e que versam sobre a temática, tais como a Lei nº 6.782/2020 do Distrito Federal.

Foram analisadas notas técnicas do LAPIN (2021) e relatórios sobre IA, privacidade, RF, proteção de dados pessoais feitas pelo ITS Rio (2020) bem como pelo Instituto de Pesquisa Data Privacy Brasil (DATA PRIVACY BRASIL RESEARCH, 2022), Observatório de Segurança Pública (2020) e Centro de Estudos de Segurança e Cidadania (2019).

Ainda, foram assistidos documentários e filmes que tratam sobre a temática do RF e da privacidade e proteção de dados pessoais, com destaque para *Coded Bias* – Diretora: Shalini Kantaya, Netflix (CODED BIAS, 2020) e o filme *1984: o futuro do mundo*, baseado no livro *1984*, de George Orwell, escrito por Nade Judge, bem como por postagens em redes sociais, tais como Linkedin, Instagram, YouTube e Twitter.

O presente trabalho também obteve contribuições de palestras em Fóruns de Segurança Pública, Núcleo de Estudos sobre Violência da Universidade de São Paulo e Núcleo de Estudos em Segurança Pública da UFBA disponibilizados na internet – YouTube – em seus sites institucionais.

No aspecto internacional, mereceu destaque a pesquisa sobre instrumentos normativos que tratavam sobre os direitos fundamentais da privacidade e proteção de dados pessoais, bem como as normatizações sobre a utilização da IA de RF pela administração pública e iniciativa privada, com ênfase para a utilização na segurança pública.

Assim, diplomas internacionais trouxeram suporte legal e técnico ao norte da pesquisa, são eles: Declaração Universal de Direitos Humanos (DUDH), no que tange ao direito fundamental da privacidade, e o GDPR – Diretiva nº 2016/679, no que se refere a uma abordagem de respeito ao tratamento dos dados pessoais e a livre circulação destes – *data free flow* – na Europa. Trazer essa legislação europeia para a pesquisa se tornou importante, haja vista ter sido o espelho da legislação sobre proteção de dados pessoais brasileira (PECK, 2020).

Ainda se destaca a diretiva da UE 680/2016 com suas normas específicas sobre o tratamento dos dados pessoais para fins prevenção, investigação e repressão para fins penais.

Quanto à aplicação da tecnologia de IA, foram abordadas as disposições da proposta de regulação da IA da Comissão Europeia nº 2021/006 que tenta regulamentar o uso dessa tecnologia abordando as principais disposições legais.

Por outro lado, também foram estudados posicionamentos de recomendação de banimento do RF para fins de segurança pública, previstas nas Diretivas 3/2019 do EDPB e a *Ordinance* nº 107-19 da cidade de São Francisco, Califórnia, EUA, e entidade de defesa dos direitos humanos.

A escolha da *Ordinance* nº 107-19 da cidade de São Francisco se deu em razão de ser o local onde se localiza o Vale do Silício, **berço** das novas tecnologias, mas que foi o primeiro local do mundo a ter uma legislação proibindo a utilização do RF para segurança pública.

7.1 ORGANIZAÇÃO DO MATERIAL: PROCEDIMENTOS DA ANÁLISE DOCUMENTAL

Os materiais coletados nas bibliotecas físicas e digitais, bem como nos sítios eletrônicos diversos foram organizados em pastas físicas e digitais, o que ajudou no processamento da leitura para a realização da análise do conteúdo.

Para tanto, foi feita, sinteticamente, a seguinte organização, no tocante aos livros físicos, digitais, artigos científicos, dissertações e teses, revistas e periódicos: foram anotadas as referências completas, como número de páginas, endereço eletrônico ou indicação do livro ou revista onde foi encontrada, ano de publicação, respectiva identificação catalográfica, resumo e citações de alguns trechos e realizadas pesquisas através de palavras-chave.

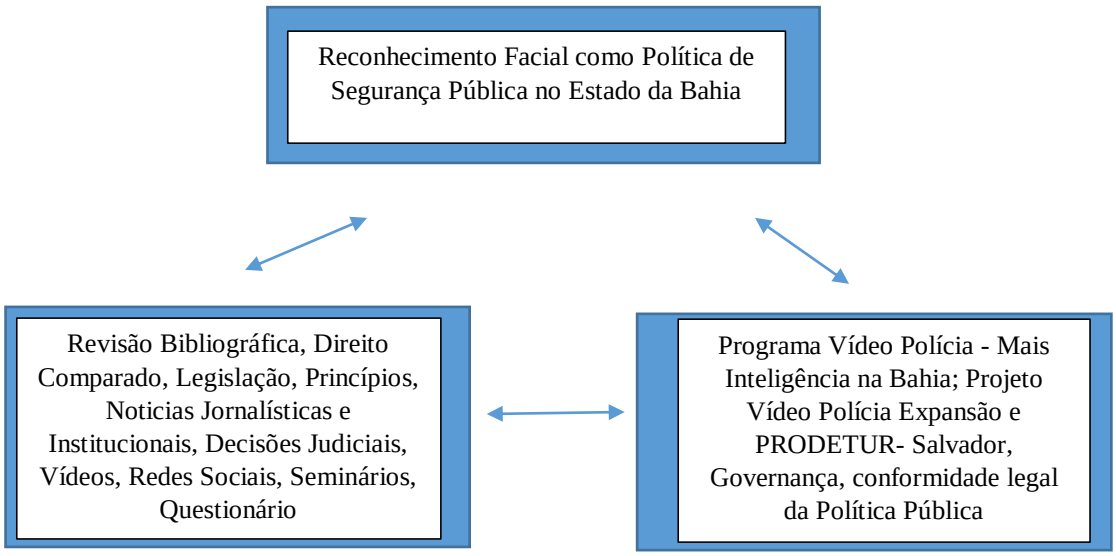
No tocante às notícias jornalísticas, materiais institucionais do governo, vídeos, postagem em redes sociais foram coletados materiais para a pesquisa em redes sociais, tais como Linkedin, Instagram, YouTube e Twitter, através de acompanhamento das postagens de autores que foram consultados na pesquisa. Foram tirados *prints* das telas de acesso, realizada pelo computador ou smartphone, indicado o ano de publicação, resumo e citações de alguns trechos, quanto às matérias relacionadas ao tema da pesquisa, verificadas através de palavras-chave.

7.2 ESTUDO DE CASO

O estudo de caso poderá ser aplicado em diversas áreas de conhecimento e se desenvolve mediante um estudo aprofundado sobre o objeto, que poderá ser entendido como indivíduo, organização, grupo ou fenômeno (SILVEIRA; CÓRDOVA, 2009, p. 34).

Para Yin (2005, p.32), “o estudo de caso é uma investigação empírica que investiga um fenômeno contemporâneo dentro de seu contexto da vida real”. No Fluxograma 1, pretende-se demostrar o estudo de caso a ser estudado, com suas principais fontes de extração dos dados através de revisão bibliográfica que contribui para a formação do referencial teórico e na categorização e análise dos dados coletados.

Fluxograma 1 – Estudo de caso



Fonte: Elaborado pela autora (2022).

Na pesquisa está sendo trazida à baila políticas públicas específicas do Estado da Bahia, denominadas Projeto Vídeo Policiamento – Mais Inteligência na Segurança e Projeto Vídeo-Polícia Expansão, que, em 2018, mediante realização de aditivo contratual, deu origem à inclusão do RF como política de segurança pública e ainda o PRODETUR - Salvador, criado pelo Município de Salvador e que utiliza o RF como política de segurança turística.

Para tanto, foram coletados o termo de referência da licitação, justificativas técnicas da contratação das câmeras e da tecnologia de videomonitoramento por RF pelo governo da Bahia e município de Salvador, bem como informações sobre a empresa vencedora da licitação que autorizou os serviços de monitoramento.

Destaca-se que, ao pesquisar sobre a aplicação da política pública de RF do Estado da Bahia, o recorte da pesquisa teve natureza de pesquisa aplicada, na medida em que apresentou dentre os seus escopos gerar conhecimentos práticos, com soluções específicas e com interesses locais (SILVEIRA; CÓRDOVA, 2009, p. 35).

Tratar da pesquisa com recorte geográfico para o Estado da Bahia é vislumbrar a possibilidade do trabalho contribuir na forma de ações propositivas de avaliação da política pública de RF já em andamento.

Ainda, foram compiladas as notícias jornalísticas, vídeos dos líderes estaduais do projeto de RF na Bahia falando sobre o pioneirismo da Bahia na aplicação do RF na segurança pública e a sua repercussão no Brasil e no mundo.

7.2.1 Aplicação de Questionário

Para coleta de dados na pesquisa foi utilizado a aplicação do questionário (APÊNDICE A) que, segundo Gil (2002), é uma técnica de investigação composta por questões apresentadas por escrito às pessoas, com o escopo de conhecer, por exemplo, opiniões, crenças, interesses, e situações vivenciadas.

O objetivo da adoção do questionário foi conhecer de que forma o Estado da Bahia está disponibilizando os dados e informações relativas à política pública de RF aplicada a segurança no Estado, se está havendo transparência nas disposições dos dados sobre a política.

Ainda, objetivou-se identificar a existência de erros quanto à aplicação da tecnologia de RF automatizado na identificação de pessoas e que puderam levar a prisão de inocentes como também analisar qual justificativa técnica ou legal foi utilizada para a adoção desse mecanismo tecnológico como uma política pública.

Para Quivy e Campenhoudt (2004, p. 188), "o inquérito por questionário de perspectiva sociológica distingue-se da simples sondagem de opinião pelo fato de visar a verificação de hipóteses teóricas e a análise das correlações que essas hipóteses sugerem". Assim, o objetivo do método é analisar um fenômeno social que se pretende melhor estudar a partir de informações da população a ser estudada.

Para consecução da pesquisa foi apresentado um questionário à Ouvidoria Geral do Estado da Bahia, mediante preenchimento de requerimento no sítio eletrônico: http://www.ouvidoria.ba.gov.br/, no dia 03 de novembro de 2021, contendo dez questões por escrito, de forma aberta, com roteiro de perguntas previamente estabelecidas, que versaram sobre a aplicação da tecnologia de RF como política de segurança pública do Estado da Bahia.

Segundo Chaer, Diniz e Ribeiro (2011, p. 253), "as perguntas abertas são aquelas que permitem liberdade ilimitada de respostas ao informante", com a vantagem do respondente não sofrer influência do pesquisador". Além disso, os pesquisadores da área qualitativa preferem as perguntas abertas ressaltando a relatividade cultural das palavras para aquela circunstância perguntada (VIEIRA, 2009).

A escolha pelas questões abertas foi realizada, tendo em vista que se pode buscar, na resposta dos respondentes, boas e novas ideias para a discussão do trabalho, bem como apresenta ainda, como vantagens, a possibilidade de indicação de informação do respondente e permite que os respondentes expressem as respostas com suas próprias palavras (VIEIRA, 2009).

As perguntas do questionário (APÊNDICE A) foram enviadas, via e-mail, invocando a LAI, Lei nº 12.527/2011, recebidas pela Ouvidoria Geral do Estado da Bahia e confirmadas à pesquisadora, por meio de e-mail de recebimento da manifestação nº 2502646, protocolada sob o nº 409, no dia 03 de novembro de 2021. Segundo o e-mail, a solicitação foi encaminhada para a Superintendência Gestão e Tecnologia Organizacional, através do Ofício nº 1.058, para conhecimento e providências.

No dia 10 de novembro de 2021, foi recebido pela pesquisadora, um e-mail da Ouvidoria Geral de Polícia/SSP-BA que apresentou as respostas do questionário supramencionado, pela Assessoria Técnica – SSP/GAB/SGTO/ASTEC.

É importante destacar, entretanto, que o envio de questionário de autoaplicação, por e-mail, também apresentou limitações metodológicas, visto que a pesquisadora sabe o setor que respondeu às perguntas, mas não a pessoa específica, contudo, em comparação com suas vantagens, as respostas apresentadas se mostraram bastante úteis e importantes para efeito da pesquisa.

8 RECONHECIMENTO FACIAL COMO POLÍTICA DE SEGURANÇA PÚBLICA NO ESTADO DA BAHIA

O presente capítulo tratará sobre o estudo de caso referente a aplicação das câmeras de viodemonitoramento por RF via IA como política de segurança pública no Estado da Bahia.

Inicialmente será realizado um breve histórico sobre o videomonitoramento na segurança pública do Estado da Bahia, desde o CFTV até os dias atuais com o RF automatizado.

Posteriormente, serão trazidos à baila exposição sobre os projetos Vídeo Policiamento – Mais Inteligência na Segurança, Vídeo-Polícia Expansão e PRODETUR Salvador. Após a breve exposição sobre os programas acima, será tratado o RF com relação a (in)existência de falso-positivos.

O trabalho continuará apresentando dados sobre as decisões proferidas pelo poder judiciário sobre a multirreferida política pública no Estado da Bahia no Tribunal de Justiça da Bahia (TJ-BA) e Tribunais Superiores.

Por fim, o capítulo tratará sobre a análise e discussão dos dados coletados, que embasam o trabalho e fundamentam a realização da pesquisa acadêmica, de forma a demonstrar as vantagens e riscos de aplicação do RF como política de segurança pública no Estado da Bahia.

8.1 DO VIDEOMONITORAMENTO POR CFTV AO RECONHECIMENTO FACIAL POR INTELIGÊNCIA ARTIFICIAL

O registro da instalação do videomonitoramento – CFTV urbano na cidade de Salvador, Bahia, remonta ao início dos anos 2000, quando foram instaladas câmeras de segurança vinculadas a pontos policiais no circuito do Carnaval, orla e centro da cidade. A SSP-BA ficava responsável pela instalação das câmeras e os policiais militares pelo manuseio dos equipamentos (FREITAS FILHO, 2018).

Não havia compartilhamento das imagens entre o ponto da instalação e outros centros. As imagens eram armazenadas em fitas *Video Home System* (VHS), recolhidas pelos policiais ao final dos turnos e enviadas para uma ilha de edição, localizada na Coordenadoria de Missões Especiais (CME), para que pudesse ser procedida a análise do material pelos órgãos públicos envolvidos com a organização do Carnaval (FREITAS FILHO, 2018).

O sistema de videomonitoramento – CFTV de áreas públicas de forma integrada foi realizada em Salvador, no Centro Histórico do Pelourinho, em 2007, através da instalação de 14 câmeras analógicas de vídeos, instaladas via cabos *Unshield Twisted Par* (UTP) à Central de Operações do 18º Batalhão de Polícia Militar da Bahia, contudo durou pouco mais de um

ano e foi descontinuado em razão de diversos problemas, desde a queda de energia que apagava as câmeras até a falta de capacitação dos policiais na operação dos equipamentos (FREITAS FILHO, 2018).

No Estado da Bahia, destacaram-se os municípios de Camaçari, Vitória da Conquista, Teixeira de Freitas, Jequié e Feira de Santana que também apresentaram sistemas de videomonitoramento em 2007, todavia o sistema foi descontinuado em razão de registros de falhas pela falta de nitidez das imagens captadas (FREITAS FILHO, 2018).

Em 2008, foi montado um novo projeto de videomonitoramento para o Carnaval de Salvador, desta vez com transmissão das imagens para uma central instalada na Superintendência de Inteligência da SSP-BA, via ondas de rádios, mas que sofreram diversas interferências das transmissões de TV e rádios que utilizavam o mesmo canal, dificultando a operacionalização (FREITAS FILHO, 2018).

Em 2010 e 2011, a SSP-BA instalou cabos de fibra óptica no circuito do Carnaval de Salvador, o que melhorou a eficiência do sistema, mas ficou marcado pela dificuldade de capacitação dos policiais para utilizarem a tecnologia (FREITAS FILHO, 2018).

Em 2012, em razão do estímulo ao videomonitoramento, através da possibilidade de captação de recursos do Fundo Nacional da Segurança Pública do Governo Federal, foram instaladas 215 câmeras de vídeos na cidade de Salvador a serem monitoradas pelas Centrais de Unidades de Controle Policial, transmitida para a Central de Telecomunicações (CENTEL) da SSP-BA, em que as imagens eram transferidas para direcionamento de viaturas e atendimento das demandas de segurança (BAHIA, 2009).

A vinda de grandes eventos esportivos para o Brasil, como a Copa das Confederações, em 2013, e a Copa do Mundo, em 2014, contribuíram para a criação no âmbito do Ministério da Justiça, da Secretaria Extraordinária para Grandes Eventos (SESGE) ainda em 2011, que ficou responsável pela segurança pública nos eventos e de interlocução com as Secretarias de Segurança Pública dos estados da federação (PIRESet al, 2021).

Em razão disso, na Bahia foi criado, em 2012, o Centro Integrado de Gestão de Emergência (CIGE), que foi o articulador da criação do Parque Tecnológico da Bahia e da construção e manutenção de nove centros de comunicação, um investimento de R$ 95 milhões resultante de recursos dos Governos Federal, Estadual e Municipal (BAHIA, 2013; PIRES et al, 2021), consoante Figura 6:

Figura 6 – Parque Tecnológico da Bahia

Foto: Paula Fróes/GOVBA.

Fonte: BAHIA (2020).

O projeto de instalação de câmeras de videomonitoramento foi ampliado em 2013 em razão da Copa das Confederações, mediante a instalação em Salvador de mais 178 câmeras da própria SSP-BA, mais 30 câmeras do entorno e 25 câmeras dos estádios que receberam os jogos de futebol, quais sejam Arena Fonte Nova e Estádio de Pituaçu. Ainda, foram instaladas câmeras nas cidades de Porto Seguro, Bahia, em razão de terem sido escolhidas como sede para as seleções da Alemanha e Suíça para a Copa do Mundo de 2014 (FREITAS FILHO, 2018).

Esse videomonitoramento se utilizava de

> soluções de transmissão (enlaces de rádio de fibra óptica), câmeras digitais, equipamentos, ativos de rede servidores, [...] sistemas operacionais, software de gerenciamento e gravação de imagens em salas de monitoramento do Centro Integrado de Comando e Controle Regional (CICCR). (FREITAS FILHO, 2018, p. 66).

Dentro do projeto ainda foram distribuídos mais de 80 câmeras e computadores de bordo para serem instaladas nas viaturas dos policiais para atendimento em tempo real das demandas policiais e consulta de dados sobre veículos roubados (R7, 2014).

Em 2016, foi instituído o Centro de Operações e Inteligência 2 de Julho (COI), conforme Figura 7, que incorporou o CICCR, 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, mediante a publicação do Decreto Estadual nº 16.852/2016.

O Decreto Estadual nº 16.852/2016 estabeleceu, dentre outras disposições de atribuição do COI, fortalecer e integrar as forças de segurança pública e defesa civil com recursos tecnológicos para tomadas de decisões conjuntas – artigo 2º, inciso I, bem como se utilizar de equipamentos tecnológicos de última geração capazes de promover uma imagem fiel e em tempo real do panorama global – artigo 2º, inciso IV (BAHIA, 2016a).

Ainda, o Decreto Estadual nº 16.852/2016 dispôs de que seria utilizado uma **solução integradora** capaz de aglutinar sistemas de informação, comunicação e videomonitoramento viabilizando a interoperabilidade do sistema.

Figura 7 – Centro de Operações e Inteligência Dois de Julho

Videowall, no prédio do COI, no CAB.

Fonte: Freitas Filho (2018, p. 72).

O legado dos equipamentos adquiridos e os programas de segurança pública desenvolvidos na Bahia para a Copa das Confederações em 2013 e Copa do Mundo de 2014, além do Decreto nº 16.852/2016 que institui o COI, atuaram como percussores dos projetos Vídeo Policiamento – Mais Inteligência na Segurança e Vídeo-Polícia Expansão de essencial compreensão para o presente trabalho, haja vista que foi incluído nesses projetos a adoção do RF como política de segurança pública no Estado da Bahia.

Para investigação sobre os projetos acima mencionados foi utilizado como método de pesquisa um questionário (APÊNDICE A), contendo dez perguntas de respostas abertas, endereçado via e-mail à Ouvidoria Geral do Estado da Bahia em 03 de novembro de 2021 e respondido pela Ouvidoria Geral de Polícia da SSP-BA, no dia 10 de novembro de 2021, através 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.

A fundamentação do envio do questionário para acesso aos dados sobre a implantação da política pública de RF baseou-se na LAI, Lei nº 12.257/2011, em que as respostas serão melhor detalhadas a partir dos tópicos que seguem.

8.1.1 Projeto Vídeo Policiamento – Mais Inteligência na Segurança

Em 18 de dezembro de 2018, como continuidade ao projeto de videomonitoramento para fins de segurança pública no Estado da Bahia, foi lançado o Projeto Vídeo Policiamento – Mais Inteligência na Segurança pelo Governador da Bahia, Rui Costa, cuja finalidade foi agregar agilidade e IA ao sistema de viodemonitoramento já existente no estado (BAHIA, 2018), "produzindo resultado não somente para o Segmento de Segurança Pública, mas também para atendimento [...] [aos Serviços de Atendimento ao Cidadão (SAC)], unidades de saúde e escolas bem como a integração com sistemas de vídeo monitoramento de prefeituras e da iniciativa privada" (BAHIA, 2019h, p. 16).

O projeto foi lançado ao custo de investimento de R$ 18 milhões e ainda permitiu a implementação de ferramenta de pesquisa de registro, para traçar trajetórias de pessoas ou veículos enquadrados ou não como suspeitos, bem como realizar análise situacional de trechos de gravação das câmeras (BAHIA, 2021a).

Segundo a SSP-BA, a tecnologia de videomonitoramento capta as imagens e as encaminha para os pontos de recebimento que analisa os rostos captados, mediante cruzamento com bancos de dados de mandados de prisão. O Centro Integrado de Comunicações (COE) recebe e gera os alertas dos sistemas, além de acionar as equipes de policiais mais próximas para verificação de veracidade do RF e adoção de providências (BAHIA 2021b).

O sistema estreou no Réveillon de Salvador, em 27 de dezembro de 2018, mediante a instalação de 50 câmeras de RF (BAHIA, 2018) e conta com 60 terabytes de processamento de imagens, o que significa a análise de até duas mil imagens de forma simultânea (BAHIA, 2018).

Sob o aspecto técnico, em resposta à pergunta nº 1 do questionário (2021), quanto ao requerimento de informações técnicas sobre o RF utilizado pela SSP-BA, a Assessoria Técnica – SSP/GAB/SGTO/ASTEC, assim se manifestou:

> a solução de vídeo analítico avançado, implantada em 2018, possui uma arquitetura flexível e que permite o uso de algoritmos de analises em câmeras IP, com condições para que o usuário defina os gatilhos de eventos para um alarme, o que contribuiu para

> a automatização de diversos processos realizados anteriormente de forma manual, otimizando seus resultados. Essa solução foi desenhada visando a alta disponibilidade dos serviços, com configuração em modo Cluster ativo-ativo, instalada no Data Center do Centro de Operações e Inteligência (COI), com acesso restrito ao ambiente. No que tange ao Reconhecimento Facial, o uso de suas licenças é feita de acordo com pontos de interesse de monitoramento por parte da Segurança Pública, visto que esses analíticos podem ser direcionados, a qualquer momento, para qualquer câmera da SSP, desde que atendam aos requisitos técnicos de configuração. Registra-se que o uso da Tecnologia de Reconhecimento Facial pela Segurança Pública visa apoiá-la no exercício das atribuições legais das forças policiais como a proteção da vida e da propriedade, prevenção e detecção de crimes e garantia da segurança pública, tornando-se um instrumento salutar para o combate à criminalidade e passando a ser um instrumento agregador no mecanismo de prevenção ao crime quando empregadas em conjunto com processos e práticas eficientes de policiamento. (QUESTIONÁRIO, 2021).

O projeto Vídeo Policiamento – Mais Inteligência na Segurança foi implementado via licitação em que foi celebrado o Contrato nº 002/2014/DG/SSP-RDC1, Consórcio Projeto CIGE Bahia, tendo como líder a empresa El Corte Inglês (IECISA), "cujo escopo foi a prestação de serviço para equipar tecnologicamente a SSP-BA, de forma a compor o CIGE, hoje denominado COI" – Resposta nº 2 do questionário (2021).

Importante ressaltar que o RF, via IA, foi incluído no projeto Vídeo Policiamento – Mais Inteligência na Segurança, através da realização de um aditivo contratual que 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, todas com a capacidade de sinopse e analise forense e que foram fornecidas pela empresa Huawei" – Resposta 2 ao questionário (2021).

O consórcio liderado pela IECISA contratou a empresa Huawei Enterprise no Brasil, líder global de soluções de TICs, para entregar a tecnologia utilizada no RF – Resposta 2 ao questionário (2021). A empresa chinesa foi fundada em 1987 e tem sua origem na cidade de Shenzhen, na China (HUAWEI, 2022).

Segundo o Diretor de Marketing da Huawei, Rômulo Horta, em uma entrevista por vídeo ao site Convergência Digital (PRESCOTT e MARIANO, 2018), a tecnologia fornecida pela Huawei ao Estado da Bahia opera por *VideoCloud*, ou seja, é um "sistema de vídeo analítico que tem capacidade de fazer RF, contagem de pessoas, leitura de placa de veículos", cuja função seria integrar os sistemas independentes de videomonitoramento da SSP-BA com as 1900 câmeras já instaladas na cidade de Salvador, em locais como rodoviária, estações de metrô, ferryboat, aeroporto, Elevador Lacerda e em estádios de futebol, a fim de garantir que o gerenciamento dessa integração possa ser feito pela SSP-BA (PRESCOTT; MARIANO, 2018).

Quanto à operacionalização do *VideoCloud*, segundo resposta ao item 4 do questionário (2021) apresentado, sobre quais bases de dados são utilizadas para análise do RF na Bahia, a Assessoria Técnica-SSP/GAB/SGTO/ASTEC informou que as bases de dados "utilizadas para aplicação do comparativo para o RF são os bancos de dados de procurados com mandado de prisão e desaparecidos, de fonte exclusiva da SSP-BA, instalada no COI e alimentada pela Superintendência de Inteligência". Em 2019, a base de dados da SSP-BA era de aproximadamente 65 mil imagens, consoante informação do então Secretário da SSP-BA à época, Maurício Barbosa (G1, 2019).

Ainda, cumpre observar que o Superintendente de Gestão Tecnológica da SSP-BA, Coronel Marcos Oliveira, informou, em 2019, que também constavam, no banco de dados de informações da SSP-BA para o cruzamento de informações, imagens de pessoas retiradas de redes sociais e que, inclusive, fez um teste de RF com o repórter Salviano, do programa de televisão Fantástico da TV Globo, que fazia uma reportagem sobre a implantação do RF na Bahia (G1, 2019).

O repórter do Fantástico, que nunca tinha vindo à Bahia e não constava na lista de foragidos ou com mandados de prisão em aberto da SSP-BA, ao passar pelo aeroporto de Salvador, foi reconhecido pelas câmeras, através de um cruzamento com fotos de suas redes sociais (G1, 2019). Ao site Intercept, em 2021, o Coronel Marcos Oliveira confirmou que policias se utilizam de imagens públicas das redes sociais para fazer investigação de algum crime (FALCÃO, 2021).

Importante observar que em 2021 foi informado pela SSP-BA que para consulta das pessoas a serem identificadas pelo RF também eram consultados à Base Nacional de Mandados de Prisão e Foragidos do CNJ, o BNMP 2.0 (PIRES et al, 2021).

Quanto ao critério de análise, o projeto Vídeo Policiamento – Mais Inteligência na Segurança trabalha com condições de similaridade entre o banco de dados da SSP e o suspeito com abordagem policial com condições acima de 90%, com protocolo operacional previamente definido e de forma complementar é utilizado um critério subjetivo na abordagem policial para permitir a veracidade dos dados do alerta do sistema evitando constrangimentos desnecessários – Resposta 6 ao questionário (2021).

Na hipótese do sistema detectar "uma pessoa que tenha alguma restrição, como mandado de prisão ou desaparecidos, a ferramenta emite um alerta ao Centro Integrado de Telecomunicações (CICOM), que aciona uma equipe policial mais próxima do local para realização de abordagem e tomar as devidas ações" - Resposta 6 ao questionário (2021).

A primeira prisão, via RF por IA, aconteceu no Carnaval de Salvador, no dia 05 de março de 2019, e teve grande repercussão na imprensa nacional e internacional pela identificação de Marcos Vinicius, 19 anos, mesmo ele estando travestido de mulher para participação em um bloco de carnaval, conforme Figura 8. O suspeito estava com um mandado de prisão em aberto por homicídio desde 2018. Quando da utilização do RF no Carnaval de 2019 em Salvador, o sistema realizou o reconhecimento de 460 mil pessoas por dia que transitaram nos circuitos da festa (BAHIA, 2019e; MUNIZ, 2019).

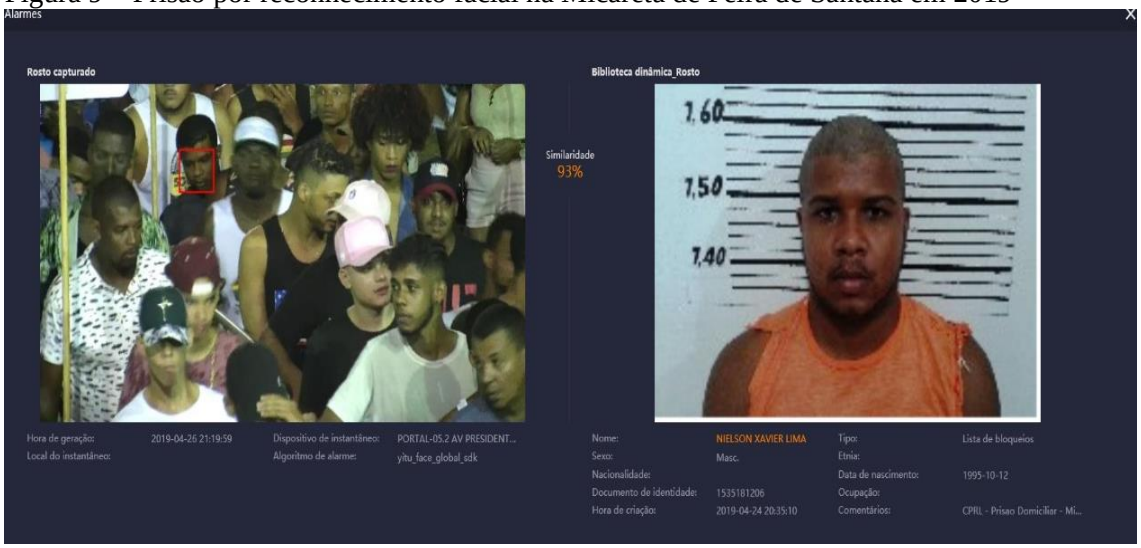
Figura 8 – Prisão por reconhecimento facial no Carnaval de Salvador de 2019

Fonte: Bahia (2019e).

O RF inteligente também foi utilizado na Micareta de Feira de Santana em 2019, que resultou na prisão de 33 pessoas com mandados de prisão em aberto ou foragidos da justiça por crimes como homicídio e tráfico de drogas. Foram reconhecidos 1,8 milhões de rostos de pessoas em quatro dias de festa (BAHIA, 2019f).

O sistema disparou 903 alertas, sendo cumpridos 18 mandados de prisão, mais a captura de 14 pessoas que descumpriam a prisão domiciliar e uma outra pessoa que já havia sido condenada pela justiça, dentre elas Nelson Xavier Lima (Figura 9), com reconhecimento com índice de 93% de similaridade (BAHIA, 2019f):

Figura 9 – Prisão por reconhecimento facial na Micareta de Feira de Santana em 2019



Fonte: Bahia (2019f).

Em 14 de maio de 2019, o Governador da Bahia Rui Costa foi apresentar no Fórum *Smart City* na cidade de Shenzhen, na China, a convite da Huawei, a política de RF na segurança pública da Bahia, como uma *case* de sucesso e destacou as prisões realizadas em razão da tecnologia no Carnaval de Salvador e no Micareta de Feira de Santana no referido ano (BAHIA, 2019a).

Em 17 de setembro de 2019, no primeiro ano de funcionamento do RF, a SSP-BA ganhou o Prêmio Case de Sucesso na 12ª edição do 4CIO Bahia, *Chief Information Officer*, promovido pela organização *Internet Technology Four* (IT4CIO) (BAHIA, 2019g; ANDRADE, 2019).

Na ocasião, o Superintendente de Gestão Tecnológica e Organizacional da SSP-BA, Coronel PM Marcos Oliveira afirmou que o prêmio fortalecia o desejo da instituição pública em ampliar o projeto e o Secretário de Segurança Pública da época, Maurício Barbosa, declarou que a comunidade tinha a ganhar com o RF, tendo em vista o menor tempo de resposta e segurança (BAHIA, 2019g).

No primeiro ano da implementação da política de RF foram identificadas e presas, na Bahia, 96 pessoas que tinham mandados de prisão em aberto ou estavam foragidas da justiça brasileira, entre os quais 15 homicidas, 19 traficantes, 22 assaltantes, além de estupradores, agressores e outros foragidos por crimes diversos, fato este muito comemorado pela SSP-BA (BAHIA, 2019b).

Em janeiro de 2020 foram divulgados pela SSP-BA dados que revelavam que a Bahia alcançou quase 26% de redução em crimes de roubos de bancos, apresentando decréscimo

também nos índices de outros crimes contra o patrimônio, com desafios ao crescente aumento dos crimes contra a vida no Estado. O sucesso da redução da criminalidade foi atribuído às ações de inteligência da polícia e à utilização da tecnologia de videomonitoramento (BAHIA, 2020b).

Em 2020, para os eventos Carnaval de Salvador, Micareta de Feira de Santana e Réveillon de Salvador foi publicada uma proposta comercial para aquisição de câmeras de CFTV e para a utilização do RF em ambientes não controlados (PIRES et al, 2021).

Para essa proposta, foram expostos alguns requisitos da contratação, sendo os mais relevantes: "(i) tipo de câmera e aos (ii) pontos de recebimento de imagem. Sobre o (i) tipo de câmera, foi escolhida a *Pan, Tilt, Zoom* (PTZ), com movimentações verticais, horizontais e capacidade de aproximação da imagem, sendo ideal para o monitoramento de grandes ambientes por conta de sua versatilidade" (PIRES et al, 2021, p. 25).

Ainda no Carnaval de Salvador 2020, foi testado um aplicativo, ligado à base de dados do Instituto Pedro Melo de Identificação, denominado *Face Check*, que possibilitou em que equipes do Departamento de Polícia Técnica (DPT) realizassem a identificação de uma pessoa foragida, desaparecida ou com mandado de prisão em aberto, apontada pelo RF, em apenas um minuto (BAHIA, 2020b).

O *Face Check* é um sistema multibiométrico que pode identificar as pessoas tanto pela digital quanto pelas análises de faces. Nessa oportunidade, foram identificadas 6,5 milhões de pessoas que passaram pelos 42 portais de monitoramento da polícia militar em quatro dias do Carnaval de Salvador (BAHIA, 2020d).

Os dados biométricos coletados pelo viodemonitoramento são armazenados em servidor privado da SSP-BA e ficam hospedados no *data center* do COI no Centro Administrativo da Bahia (CAB). O acesso é limitado mediante autenticação no ambiente tecnológico e ainda assinatura de termo de confidencialidade – Resposta ao item 9 do questionário (2021).

Os dados biométricos são classificados como de acesso total restrito de sigilo e todo acesso ou qualquer alteração ou movimentação na plataforma onde estão armazenados os dados pessoais são feitas por servidor autorizado e registrado mediante *log* de acesso – Resposta ao item 9 do questionário (2021).

No que tange a possibilidade de compartilhamento dos dados biométricos com outros governos ou ainda mediante transferências internacionais, foi informado pela SSP-BA de que não há compartilhamento de dados – item 10 do questionário (2021). Segundo a Huawei, os dados coletados são criptografados e ficam com a SSP-BA, assim a empresa fica apenas

responsável pela disponibilização da plataforma tecnológica que foi adquirida pelo Estado para instalação do equipamento (PIRES et al, 2021).

Há uma preocupação quanto à segurança física das instalações do parque tecnológico onde está localizado o COI, inclusive com treinamentos pelos policias na Academia de Polícia Civil (ACADELPOL) no curso realizado de **segurança de autoridades** quanto a medidas de segurança e contrainteligência para a preservação de locais de produção de conhecimento e dados sensíveis, sistema, videomonitoramento com o uso de tecnologia, CFTV e sistema de videmonitoramento inteligente (BAHIA, 2021b).

Até novembro de 2021, quando do envio das respostas do questionário (APÊNCIE A) apresentado à SSP-BA, já haviam sido identificadas e presas 221 pessoas – Resposta ao item 3 do questionário (2021), inclusive um foragido utilizando máscara de proteção contra a Covid-19 (BAHIA, 2020e).

Segundo o Coronel Marcos Oliveira, em entrevista ao Jornal Correio, em 5 de janeiro de 2020, quanto a ser questionado sobre a maioria das pessoas presas através do RF serem pretas ou pardas, ele respondeu que isso ocorre não porque há um possível racismo da ferramenta tecnológica, mas sim porque mais de 80% das pessoas na Bahia se autodeclaram pretas e pardas, portanto "o sistema vai em cima de coisas que são fáticas: se a pessoa tem mandado de prisão, se está desaparecida. Num estado que tem 80% da população negra, é quase uma lógica que vai ser maioria" (PALMA; PACHECO, 2020).

Sobre a utilização de meios de participação pública prévios quanto à implementação do RF, a Assessoria Técnica-SSP/GAB/SGTO/ASTEC apresentou resposta ao item 8 do questionário (2021) de que "inicialmente no projeto Vídeo Policiamento – Mais Inteligência na Segurança foi feito um piloto com o uso dessa ferramenta que apresentou resultados exitosos para a sua finalidade de aplicação.

Em razão da apresentação do RF como *case* de sucesso, desde 2019, o Governador da Bahia já afirmava estar feliz com o resultado do "projeto piloto que proporcionou mais segurança aos baianos" (BAHIA, 2019a) e de que havia um projeto de expansão, mediante a licitação de instalação de câmeras de RF para mais 55 cidades do Estado da Bahia, a fim de melhorar a ampliação de serviços para a população (BAHIA, 2019a). A expansão do programa Vídeo-Policiamento – Mais Inteligência na Segurança ocorreu mediante a publicação de um projeto complementar chamado de Vídeo-Polícia Expansão.

8.1.2 Projeto Vídeo-Polícia Expansão

Em 2019, como continuidade ao projeto de ampliação do videomonitoramento por RF na segurança pública do Estado da Bahia, foi publicado o termo de referência da licitação do projeto denominado Vídeo-Polícia Expansão, cujo objeto foi a contratação de pessoa jurídica "para prestar serviços integrados, sob demanda, voltados a ponto de imagem em locais de interesse, monitoramento, sustentação e atualização de infraestrutura de operações e provimento de comunicação móvel crítica com banda larga" (BAHIA, 2019h, p. 5).

Nesse esteio, a contratação acima seria para expansão do videomonitoramento por RF em áreas públicas para 78 municípios do Estado da Bahia. Dentro dos pontos de imagem descritos na Tabela 1 do item 1.1 do termo de referência, se destacam monitoramento do CICOM, passeios públicos, avenidas, praças de convivência pública, com suporte a análise comportamental, situacional, ambientes internos e externos de fluxo livre com suporte para RF, área de orla com suporte de reconhecimento de placas e veículos, dentre outros (BAHIA, 2019h).

Importante ressalvar que, para a fase de expansão do videomonitoramento, via RF, foi realizada audiência pública, com divulgação de avisos e resumos dos editais de licitação no Diário Oficial do Estado (DOE) e em jornais de grande circulação, conforme determina o artigo 54 da Lei de Licitações Estadual nº 9.433 – Resposta ao item 8 do questionário (2021).

A justificativa da expansão do projeto ocorreu em razão da viabilização das previsões do Decreto nº 16.852/2016, que instituiu o COI e cuja finalidade foi a transversalidade e integração das ações operacionais da segurança pública, com soluções tecnológicas integradoras. O certame permitiu a participação de consórcios de empresas (item 3.2.2.1) e a possibilidade de subcontratação (item 3.3.2.1) e estabeleceu um prazo de 60 meses por se tratar de serviços contínuos, de alta complexidade e grande vulto (item 3.2.5.1).

A justificativa da contratação ocorreu sob a narrativa de melhoria da prestação de novos serviços públicos, mediante novos modelos de gestão, superação de mão de obra qualificada para áreas críticas de tecnologia, bem como prazos de insumos, equipamentos e ainda sem preocupações com manutenção dos equipamentos, celeridade na reposição de peças, conservação de ativos, uma vez que a administração pública teria serviços e produtos com tecnologia de ponta, integrados aos sistemas, mas apenas exercendo sua função de fiscalização da qualidade, eficiência e prestabilidade da execução dos serviços (BAHIA, 2019h).

Quanto à justificativa da contratação do ponto de imagem (videomonitoramento), foi mencionado que o projeto Vídeo Policiamento – Mais Inteligência na Segurança focou em

aquisição de câmeras e acessórios com manutenção, ao passo em que no Vídeo-Polícia Expansão seria mais vantajoso à contratação de serviços. Segundo o termo de referência (BAHIA, 2019h, p. 17):

> No modelo de contratação de serviços, o retorno do investimento é claramente percebido, uma vez que a organização mantém o foco nas atividades principais do negócio sem se preocupar com toda a infraestrutura necessária. Além disso, é altamente flexível e pode ser escalada de acordo com a necessidade da organização, permitindo um crescimento modular, de acordo com a demanda. Trata-se de uma contratação fim-a-fim. A contratação do chamado *Vídeo as a Service* (VaaS), segue uma modalidade no qual são pagas apenas mensalidades, sem a necessidade da compra dos equipamentos e de sua sustentação, onde o que é mensurável contratualmente é o resultado esperado. (BAHIA, 2019h, p. 17, grifo nosso).

Para a prestação de serviços de videomonitoramento por RF – Ponto de Imagem (PI) – não deverão ser adotadas sistemas de armazenamento de dados e nuvem – *cloud* – públicas, admitindo-se *cloud* privada, através da instalação em *data center* da SSP-BA, com exceção dos serviços de gerenciamento integrado de subsistemas de monitoramento de ambiente produtivo, auditoria e atualização que podem ser feitos de forma remota (BAHIA, 2019h).

O adendo II do termo de referência (BAHIA, 2019h) vem a estabelecer outras especificações técnicas quanto aos locais dos pontos de imagem, dividindo-o em sete tipologias, em seu item 1.3:

> Tipo 1 - Passeio público em rua ou avenida com suporte a análise comportamental/situacional; Tipo 2 - Pátios e praças de convivências externos com suporte a análise comportamental/situacional; Tipo 3 - Vias de circulação urbana de veículos e vias de transporte interurbano com suporte a reconhecimento de placa de veículo; Tipo 4 - Ambientes internos e externos de fluxo controlado, com suporte a reconhecimento facial; Tipo 5 - Ambientes internos e externos de fluxo livre, com suporte a reconhecimento facial; Tipo 6 - Áreas de orla com suporte de reconhecimento de placas de veículos e análise situacional. Tipo 7 - Panorama tático urbano. (BAHIA, 2019h).

Para os tipos de ponto de imagem 1, 2 e 3, acima mencionados, foram previstas condições analíticas de comportamento e que não devem ser confundidas com o método de aplicação do RF, quais sejam:

> o Cruzamento de Linha Vertical (CLV), que gera um alerta quando uma linha desenhada na imagem é cruzada em determinado sentido; o Controle de Fluxo Poligonal (CFP), que gera um alerta quando uma pré-condição de fluxo é atingida em um dos lados de um quadrilátero desenhado em tela; a Permanência em Área Designada (PAD), que gera um alerta quando um tempo pré-determinado é excedido por uma pessoa ou objeto que permanece em certa área delimitada; a Detecção de Ausência de Movimento (DAM), que gera um alerta quando não há movimento na

> área designada por um quadrilátero na tela por um tempo pré-determinado; os Objetos Deixados/Retirados (ODR), que gera um alerta quando um objeto é removido ou aparece em tela; a Contagem de Objeto/Pessoa (COP) que, além de fazer o que o nome indica, também identifica a saída ou entrada do objeto; a Classificação de Pessoa ou Veículo (CLS); e a Detecção de Aglomeração de Pessoas (DAP), que gera um alarme quando uma quantidade pré-determinada de pessoas for excedida em determinada área designada. (PIRES et al, 2021, p. 26).

Ainda quanto aos aspectos técnicos, o Termo de Referência de 2019 previu a incidência do RF como "detectar, capturar e reconhecer rostos das pessoas em tempo real, considerando o respectivo cenário de captura de faces, com precisão de acerto maior que 90%, em ambientes controlados e 50% para ambientes diversos" (item 2.19.1.1.1).

Apesar da margem no Termo de Referência ter sido balizada a partir de 50%, na Bahia, há recomendação quanto à abordagem policial, para se dar com índice de similaridade a partir de 90% de semelhança (BAHIA, 2019h).

A licitação para a ampliação dos serviços de reconhecimento fácil foi lançada em 2019, e, em julho de 2021, foi firmado uma parceria entre o Governo do Estado da Bahia e o conglomerado vencedor Oi e Avantia de R$ 665 milhões por cinco anos. Esse é considerado o maior investimento em segurança pública da história da Bahia, segundo o Governador do Estado Rui Costa (BAHIA, 2021a).

Na primeira fase da ampliação do videomonitoramento em 2021 se previu a expansão para 39 cidades da Bahia e os demais municípios tiveram cronograma de implantação em 2022, conforme listagem (Figura 10) abaixo (BAHIA, 2021a):

Figura 10 – Municípios abrangidos pelo reconhecimento facial em 2021 e 2022

Fonte: Bahia (2021a).

Segundo Ricardo Mandarino, Secretário de Segurança Pública da Bahia, todo o processo licitatório do projeto Vídeo-Polícia Expansão foi supervisionado pelo Tribunal de Contas do Estado (TCE-BA), Ministério Público e Procuradoria Geral do Estado da Bahia (PGE-BA) (BAHIA, 2021a).

A empresa americana Hexagon é a responsável por disponibilizar um Sistema Integrador de Missão Crítica do Projeto Vídeo-Polícia Expansão, um software que promoverá a integração de todos os sistemas da área de segurança pública, permitindo a produção de relatórios e *dashboards*, pela comunicação banda larga, ou ainda através de acesso remoto, com o objetivo de disponibilizar informações necessárias aos policiais que estão nas ruas sobre o RF aplicado. Destaca-se ainda a funcionalidade que permite atualizar sistemas de gerenciamento de despacho de viaturas e demandas via 190 (BAHIA, 2022b).

Em março de 2022 o Governo da Bahia lançou o Projeto Câmera Interativa que permite o uso de imagens cedidas pela sociedade civil para auxiliar no combate ao crime. O objetivo é complementar o projeto Vídeo-Polícia Expansão e criar uma rede colaborativa para ampliar o videomonitoramento da SSP-BA mediante acesso a câmeras residenciais, de comércio e entidades privadas que serão integradas as câmeras do Poder Público (BAHIA, 2022g).

A inclusão da iniciativa privada no programa é de forma gratuita e voluntária. As câmeras cedidas pela sociedade "que possuam contrato com um integrador, precisam estar instaladas e voltadas para as ruas e avenidas dos municípios baianos, e os fornecedores deverão enviar declaração de adesão à SSP/BA e fornecer apenas imagens de locais públicos, como ruas, avenidas, parques e afins" (BAHIA, 2022b). O Decreto Estadual autorizador do programa é o de nº 21.235, de 09 de março de 2022.

Ainda, como parte da primeira etapa do projeto de Vídeo-Polícia Expansão, em uma cerimônia que aconteceu no COI, em 14 de junho de 2022, foram entregues oficialmente pelo então Governador do Estado da Bahia, Rui Costa, e seu atual Secretário de Segurança Pública Ricardo Mandarino, mais 1200 câmeras inteligentes que passam a operar na cidade de Salvador, agregando-se as 300 câmeras já existentes, além de 160 terminais de comunicação móvel (FAROL NEWS, 2022).

Na ocasião, o Governador da Bahia afirmou que o projeto prevê a instalação de mais quatro mil câmeras em 80 municípios baianos, com ampliação dos pontos de RF e de placas de veículos, e ainda mencionou o novo modelo de comunicação entre os policiais que permite o acesso, produção e compartilhamento em formatos de áudio, vídeo e fotos em tempo real (FAROL NEWS, 2022).

No Estado da Bahia, em pesquisa realizada no dia 14 de julho de 2022, há 14.057 pessoas procuradas pela Justiça e 1.283 pessoas foragidas, consoante dados do Banco Nacional de Mandados de Prisão em aberto do CNJ (CNJ, 2022), e a utilização da expansão do projeto de videomonitoramento contempla a redução gradual desse número de foragidos e com mandados de prisão pendentes de cumprimento.

Até 30 de junho de 2022 já foram identificadas e presas 287 pessoas no Estado da Bahia (BAHIA, 2022g), com destaque para o recorde de identificação da ferramenta de RF, ocorrido em 29 de junho de 2022 que culminou com 11 prisões realizadas no mesmo dia de procurados pela Justiça nas cidades de Salvador, Alagoinhas, Feira de Santana, Camaçari, São Francisco do Conde, Simões Filho e Barreiras.

8.1.3 Programa Nacional de Desenvolvimento do Turismo - PRODETUR Salvador

Em 2020, com o objetivo de incentivo ao turismo e proteção ao turista na cidade de Salvador foi lançado o PRODETUR Salvador no âmbito da SECULT, cujo objeto foi a aquisição de equipamentos para melhoria da segurança turística. O PRODETUR Salvador obteve um financiamento do Banco Interamericano de Desenvolvimento (BID), através do Contrato de Empréstimo nº 3682/OC-BR, e estabeleceu uma Licitação Pública Nacional (LPN) nº 05/2020 para aquisição dos equipamentos.

O prazo para a execução do fornecimento e/ou serviços foi previsto em até 210 dias, e o orçamento referencial para essa licitação foi de R$ 14.600.549,99. Especificamente, o objeto requeria a apresentação de propostas para aquisição de solução de monitoramento para melhoria da segurança turística, dentre eles *appliance* de videomonitoramento, licença adicional por câmera, licença para leitura de placas de veículos (LPR), licença para RF, *appliance* de analíticos de vídeo – LPR e RF, estação de monitoramento de vídeo, ponto de captação de imagem – câmera móvel, ponto de captação de imagem – câmera fixa com IR, ponto de captação de imagem – câmera fixa dome, disco SATA para servidor CFTV.

Um dos locais a ser implementado videomonitoramento pela Prefeitura de Salvador é o Centro Histórico de Salvador - Pelourinho, com foco na limpeza urbana e fiscalização dos vendedores ambulantes, mas, segundo o projeto, as imagens podem servir à segurança pública (ALVES, 2021a).

As imagens captadas serão analisadas em uma central situada na sede da Guarda Civil Metropolitana (GCM) da cidade de Salvador e todas as pessoas que passarem pelas câmeras serão gravadas, sendo que, especificamente quanto a aplicação do RF, este será realizado pela

SSP-BA com cruzamento de dados de procurados da justiça, foragidos ou desaparecidos. Se houver mais de 90% de similaridade da face com as imagens do banco de dados consultados pela SSP-BA, a pessoa será abordada por policiais, segundo o Secretário de Cultura e Turismo de Salvador, Fábio Mota (ALVES, 2021a).

Ocorre que, em agosto de 2021, a LPN nº 005/2020 para aquisição dos equipamentos acima mencionados, foi revogada com base no artigo 49 da Lei de Licitações nº 8.666/93. A licitação foi novamente publicada, cujo *status* atual em junho de 2022 é de que se encontra aberta como LPN nº 005/2022 – Monitoramento da Segurança Turística, DOM nº 8.277, com prazo final inicial em 21/06/2022.

8.2 FALSO-POSITIVOS

A pesquisa também se debruçou com um assunto sensível, tal qual questionar à SSP-BA sobre a existência ou não de erros da tecnologia de viodeomonitoramento e RF na aplicação das ações da segurança pública da Bahia que culminaram em prisões.

A resposta da SSP-BA quanto ao questionamento acima mencionado foi de que aquele momento (novembro de 2021), a SSP-BA não tinha conhecimento de erros de identificação provocados pela ferramenta, tendo em vista o protocolo operacional utilizado para tal identificação – Resposta ao item 5 do questionário (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, houve o questionamento à SSP-BA, e a resposta foi de que até novembro de 2021, quando foi respondido o questionário a SSP-BA não havia conhecimento sobre erros de identificação provocado pela ferramenta – Resposta ao item 7 do questionário (2021).

Cumpre destacar, entretanto, que diferentemente do que foi respondido no item 7 do questionário (2021), uma matéria do Jornal Correio, datada de 05 de janeiro de 2020, obteve destaque nacional por uma notícia de um erro da ferramenta de RF da segurança pública na cidade de Salvador, em que a ferramenta confundiu um assaltante procurado com um jovem de 25 anos que tinha deficiência mental (PALMA; PACHECO, 2020).

Segundo a mãe do jovem da reportagem, a abordagem se deu de forma violenta pelos policiais que já chegaram com a arma na cabeça e nas costas do seu filho, o que provocou diversos danos morais e constrangimentos a ela e ao rapaz vítima do erro (PALMA; PACHECO, 2020).

Sobre a questão da possibilidade de existência de erros na abordagem da ferramenta de RF, o Superintendente de Gestão Tecnológica da SSP-BA, Coronel Marcos de Oliveira, afirmou em entrevista ao Jornal Correio, em 2019, de que o "direito de abordar e buscar a identificação de alguém é previsto por lei" e afirma que há a possibilidade de ocorrerem erros, haja vista que a questão "envolve uma máquina e não uma pessoa" e na hipótese da pessoa ser abordado de forma equivocada pelos policiais, em razão de alertas errados da tecnologia, isso não seria "nenhum constrangimento", uma vez que o policial "não é orientado a chegar apontando armas" (MUNIZ, 2019).

8.3 RECONHECIMENTO FACIAL DA SECRETARIA DE SEGURANÇA PÚBLICA DO ESTADO DA BAHIA NO PODER JUDICIÁRIO

Para o presente trabalho foi pesquisado nos sites dos Tribunais de Justiça da Bahia (TJ-BA), STJ e ainda do STF decisões judiciais que versassem sobre a política de videomonitoramento e RF aplicada na segurança pública da Bahia para trazer elementos do posicionamento do poder judiciário sobre a sua constitucionalidade ou não dentro do sistema regulatório brasileiro.

Os três tribunais acima foram escolhidos para a pesquisa, tendo em vista que, por competência e foro legal definido na CF de 1988, no Código de Processo Civil brasileiro e nas leis de organização judiciária[14], seriam competentes para julgamento de possíveis ações judiciais envolvendo especificamente o videomonitoramento e o RF aplicado na Bahia, que é uma política pública de abrangência local.

No âmbito do TJ-BA foram achadas três decisões que versam sobre a temática, apresentado dois resultados desfavoráveis às pessoas presas identificadas pelo RF e um resultado favorável, com decisão absolutória quanto ao reconhecimento por videomonitoramento.

Na primeira decisão, relativo ao Processo nº 8000691-28.2021.8.05.0000 – Agravo Interno em Mandado de Segurança, o Relator Desembargador Aldenilson Barbosa dos Santos negou provimento ao recurso, sob as razões de que em que pese a fundamentação de aplicabilidade da LGPD e de possíveis vieses até mesmo raciais do RF levantados pelo Advogado do Agravado, o entendimento foi de que seria inaplicável a LGPD para fins de

[14] Constituição Federal – artigo 102: competência do STF; artigo 105: competência do STJ. Código de Processo Civil – a competência de processamento e julgamento está prevista nos artigos 43 a 53.

segurança pública, além de não ter restado provado que o sistema de RF adota mecanismo de segregação racial e econômica no caso em tela.

> PODER JUDICIÁRIO TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA Seção Cível de Direito Público Processo: AGRAVO INTERNO CÍVEL n. 8000691-28.2021.8.05.0000.1. AgIntCiv Órgão Julgador: Seção Cível de Direito Público **AGRAVANTE: ALAIN AMORIM Advogado(s): ALAIN AMORIM AGRAVADO**: ESTADO DA BAHIA e outros (3) Advogado(s): ACORDÃO DIREITO PROCESSUAL CIVIL. **AGRAVO INTERNO EM MANDADO DE SEGURANÇA. INDEFERIMENTO DE LIMINAR. USO DE SOFTWARE DE RECONHECIMENTO FACIAL**. PRELIMINAR DE NÃO CONHECIMENTO. OBSERVÂNCIA AO PRINCÍPIO DA DIALETICIDADE. REJEIÇÃO. AUSÊNCIA DOS REQUISITOS PREVISTOS NO ART. 7º, INC. III DA LEI Nº 12.016/2009. **INAPLICABILIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS PARA FINS DE SEGURANÇA PÚBLICA. INDEMONSTRADO O DESVIRTUAMENTO DO USO DA APARELHAGEM. PREVALÊNCIA DO INTERESSE PÚBLICO** TUTELADO PELO ESTADO DA BAHIA. RECURSO NÃO PROVIDO. 1. Refuta-se a preliminar de não conhecimento suscitada pelo Estado da Bahia ao fundamento de afronta ao princípio de dialeticidade, [...] **2. Em que pese a reflexão, notadamente principiológica, feita na exordial do writ, sobre o risco de desvirtuamento do uso do equipamento de reconhecimento facial e sua conversão em mecanismo de segregação racial ou econômica, não houve prova de que o sistema de segurança esteja sendo adotado para tal finalidade. 3. A alegação de ineficácia da aparelhagem veio desvinculada do acervo probatório, consistindo, em verdade, numa interpretação do impetrante sobre dados e estatísticas divulgadas pelo Estado da Bahia que carecem de exame técnico. 4. Assiste razão ao Estado da Bahia quanto a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), não ser aplicável a utilização pela Administração Pública de software de reconhecimento facial com fins de utilização na segurança pública.** [...] ACORDAM os magistrados integrantes da Seção Cível de Direito Público do Estado da Bahia, por unanimidade, em rejeitar a preliminar de não conhecimento e, no mérito, NEGAR PROVIMENTO ao recurso, nos termos do voto do relator. Número do Processo: 8000691-28.2021.8.05.0000. Data de Publicação: 26/11/2021, Órgão Julgador: SECAO CÍVEL DE DIREITO PUBLICO Relator(a): ALDENILSON BARBOSA DOS SANTOS. (BRASIL, 2021c, grifos nossos).

A segunda decisão do TJ-BA, referente ao processo HC nº 8006504-70.2020.8.05.0000, cujo relator foi o Desembargador Aldenilson Barbosa dos Santos, foi publicada em 26 de novembro de 2021 e também denegou parcialmente o Habeas Corpus postulado, em razão de prisão por RF, a decisão discorre sobre os elementos da prisão, mas na ementa não há questionamento exclusivo quanto a utilização da ferramenta tecnológica ter sido o meio para a captura do foragido.

> HABEAS CORPUS CRIMINAL n. 8006504-70.2020.8.05.0000 Órgão Julgador: Primeira Câmara Criminal 1ª Turma PACIENTE: LEONARDO VINICIUS BASTOS CARNEIRO DANTAS e outros (3) IMPETRADO: JUIZ DE DIREITO DE SENHOR DO BONFIM, 1ª VARA CRIME. HABEAS CORPUS. TRÁFICO DE DROGAS E ASSOCIAÇÃO PARA O TRÁFICO. FALTA DE FUNDAMENTO NA DECISÃO QUE DECRETOU A PREVENTIVA. MATÉRIA JÁ ANALISADA EM HABEAS CORPUS ANTERIORMENTE IMPETRADO. MERA REITERAÇÃO.

> NÃO CONHECIMENTO. EXCESSO DE PRAZO. NÃO CONFIGURAÇÃO. FEITO COM TRAMITAÇÃO REGULAR. COMPLEXIDADE. PLURALIDADE DE ACUSADOS. 16 NO TOTAL. NECESSIDADE DE EXPEDIÇÃO DE PRECATÓRIA. **PACIENTE QUE PERMANECEU FORAGIDO POR DETERMINADO ESPAÇO DE TEMPO**. ORDEM PARCIALMENTE CONHECIDA E, NESTA EXTENSÃO, DENEGADA. 1. O paciente é acusado da prática dos crimes de tráfico de drogas e associação ao tráfico (arts. 33 e 35 da Lei nº 11.343/2006), por, supostamente, fazer parte de uma súcia criminosa voltada à disseminação de substâncias entorpecentes no município de Senhor do Bonfim e no Estado da Bahia, além de serem investigados pela prática de homicídios e outros delitos correlacionados ao tráfico de drogas, sendo a prisão preventiva decretada em 03/07/2019, **mas somente efetivada em 06/12/2019, em Salvador, após identificação pelo sistema de reconhecimento facial**. 2. Inicialmente, registro que a ordem deve ser parcialmente conhecida, uma vez que a legalidade do decreto preventivo já foi analisada em ação mandamental anteriormente impetrada – HC n° 8028294-47.2019.805.0000 -, [...]. ACORDAM os Desembargadores integrantes da Primeira Turma Criminal que compõe a Primeira Câmara Criminal do Tribunal de Justiça do Estado da Bahia em CONHECER PARCIALMENTE e, nesta extensão, DENEGAR a ordem, e o fazem pelas razões postas no voto do Relator. **Número do Data de Publicação:** 26/11/2021; **Relator(a):** ALDENILSON BARBOSA DOS SANTOS; **Classe:** Agravo. (BRASIL, 2021d, grifos nossos).

A terceira decisão encontrada no site do TJ-BA, se tratou-se do Processo: 0000502-16.2012.8.05.0191, acordão publicado em 15 de abril de 2014 e se referiu a improvimento de recurso de Apelação do Ministério Público da Bahia, em razão da sentença absolutória de uma pessoa que foi presa por tráfico de drogas, com base em provas de câmeras de videomonitoramento, que segundo o processo não continha elementos de nitidez suficientes para o RF do réu.

> APELAÇÃO CRIMINAL – ART. 33 DA LEI 11.343/06 – SENTENÇA ABSOLUTÓRIA – RECURSO DO MINISTÉRIO PÚBLICO – AUSÊNCIA DE CONFISSÃO – DEPOIMENTOS IMPRECISOS – INSUFICIÊNCIA PROBATÓRIA – INCIDÊNCIA DO PRINCÍPIO DO IN DUBIO PRO REO – RECURSO CONHECIDO E DESPROVIDO. I [...] II – Após exame minucioso dos autos, constata-se a ausência de prova suficiente para a condenação, razão pela qual deve ser refutada a irresignação apresentada pelo Órgão Ministerial, uma vez que o arcabouço probatório produzido durante toda a persecutio criminis não demonstrou, com a necessária segurança, ter sido o apelante o autor do crime de tráfico de drogas. III – **De acordo com os depoimentos dos agentes penitenciários Alexandre Pedro da Silva Júnior e José Evânio Lemos Alencar, verifica-se que não foi possível realizar o reconhecimento facial do recorrido, tendo em vista a baixa qualidade das imagens captadas, à noite, pelo monitor, que sequer possibilitaram a identificação precisa das vestimentas utilizadas pela pessoa que arremessou a droga para dentro do presídio.** Deve-se enfatizar, ainda, que as referidas testemunhas limitaram-se a afirmar a existência de semelhança entre o biotipo do sentenciado e do indivíduo visualizado no monitor, indício este que se mostra insuficiente para autorizar a reforma da sentença guerreada. IV – Conclui-se, portanto, que as provas produzidas revelaram-se imprecisas e deficientes para a prolação de uma condenação, que exige um juízo de certeza no espírito do Julgador, o qual não foi alcançado na hipótese sub judice, tendo em vista que o Parquet não se desincumbiu, satisfatoriamente, do seu onus probandi, conforme determina o art. 156, caput, do Código de Processo Penal. V Ante o exposto, impõe-se o CONHECIMENTO E DESPROVIMENTO do Recurso de Apelação. Número do

> Processo:0000502-16.2012.8.05.0191. Data de Publicação:15/04/2014. Órgão Julgador: SEGUNDA CAMARA CRIMINAL - SEGUNDA TURMA. Relatora: Nágila Maria Sales Brito. 15.04.2014. (BRASIL, 2014b, grifos nossos).

No âmbito do STJ foi encontrada uma decisão no Habeas Corpus nº 631298-Bahia, impetrado por Alain Amorim em face do Secretário de Segurança Pública, Comandante da Polícia Militar e o Governador do Estado da Bahia sob a alegação do impetrante de que a política de RF aplicada pela SSP-BA serviria de instrumento de vigilância para o Estado, seria uma política pública ineficiente porque, diante da quantidade de captura de rostos, o percentual efetivo de pessoas reconhecidas era muito pequeno, de que não estaria de acordo com a LGPD e nem princípios constitucionais, como a privacidade, e teria incidência maior de erros na população negra, por isso violaria o direito de ir e vir do paciente (BRASIL, 2020).

Em novembro de 2020, o Ministro Relator Joel Ilan Parcionick denegou a ordem, tendo em vista que entendeu que o impetrante queria um salvo conduto de constrangimentos e ameaças que não aconteceram e nem ficaram provadas (BRASIL, 2020).

Em pesquisa ao site institucional do STF não foram encontradas ações judiciais em curso ou já finalizadas que versassem sobre a política pública de videomonitoramento e RF estabelecida pelo Estado da Bahia até a finalização da pesquisa.

8.4 ANÁLISE DOS DADOS E DISCUSSÃO DOS RESULTADOS

Os dados coletados para a pesquisa permitiram compreender a evolução da sociedade baiana sob a espeque da valorização da informação e do videomonitoramento como ativos importantes para a consolidação de políticas públicas de segurança, a partir dos anos 2000 (FREITAS FILHO, 2018) de forma a produzir projetos de prevenção e repressão criminal de forma multiconectada e interoperável entre as polícias.

O impacto foi provocado, em grande parte, pelo desenvolvimento e expansão das TIC’s, difundidas com mais proeminência na Terceira Revolução Industrial (CASTELLS, 1999) e expandida pela Quarta Revolução Industrial, com a criação da tecnologia de IA de RF que mudaram a relação do corpo humano, através de sua integração com a máquina (SCHWAB, 2016).

Como fora anteriormente informado, a partir dos anos 2000, na Bahia, foram implementadas políticas públicas de segurança com base no videomoniotramento, via CFTV, como política pública de segurança, através de instalação de câmeras de vigilância na cidade de Salvador, especificamente no circuito do Carnaval, orla e centro da cidade, o que demonstra

o destaque da Bahia no uso da tecnologia como medida de prevenção e repressão criminal (FREITAS FILHO, 2018).

Os dados coletados permitiram verificar que essa ação do Estado da Bahia também se baseou no estímulo a inovação tecnológica e utilização das TICs, como política pública, previsto no Plano Nacional de Segurança Pública de 2000, como necessidade do Estado brasileiro desenvolver novas ações preventivas e de combate à criminalidade.

Em 2018, a Política Nacional de Segurança de 2018-2028 (BRASIL, 2019f) trouxe, especificamente, a possibilidade de utilização do RF para fins de fiscalização de fronteiras, portos, aeroportos e rodovias no Brasil, contudo, destaca-se que não foram identificadas leis específicas federais que versem sobre a utilização do RF na segurança pública.

Ainda em 2018, o RF, via IA, foi aplicado como política pública pelo Estado da Bahia, através do Projeto Vídeo Policiamento – Mais Inteligência na Segurança sem respaldo legal específico e com o escopo de se implantar ferramenta de pesquisa de registro, 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 formar o atual COI – Resposta 2 ao questionário (2021).

Ocorre que, importante trazer à baila que a utilização do RF pela SSP-BA, a partir de 2018, extrapolou os limites previstos na Política Nacional de Segurança de 2018-2028 (BRASIL, 2019f), visto que as câmeras de videomonitoramento via RF não foram instaladas para fins de fiscalização de fronteiras e em apenas locais citados no referido documento, mas também em ruas do circuito do carnaval, orla e centro da cidade de Salvador sem existir também nenhum aparato legislativo, ainda que estadual, que permitisse essa utilização da RF por IA para fins de segurança pública.

Pelos dados coletados, o que chama a atenção para a pesquisa é de que o RF, via IA, também 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 – Resposta 2 ao questionário (2021).

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 – Resposta 2 ao questionário (2021), o 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 em clara violação da privacidade e proteção de dados pessoais, como afirma Rodotá (2004) ao dispor sobre o perigo da utilização dessa tecnologia que poderia investigar o estado da alma das pessoas.

Destaca-se 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. Em resposta ao item 8 do questionário (2021), ao ser questionado quanto à referida participação popular, a resposta foi lacônica e afirmado que o projeto era piloto e que os resultados já se mostravam exitosos, o que reforça a interpretação acima apresentada.

Com o projeto Vídeo-Polícia Expansão, a partir de 2019, a utilização do RF, via IA, foi ampliada, mediante um aumento exponencial das instalações de câmeras de RF para Salvador e o interior da Bahia para 79 municípios baianos até 2022 (BAHIA, 2019h).

Um exemplo da apresentação da eficiência da ferramenta pelo Estado da Bahia foi a utilização desta na Micareta de Feira de Santana em 2019 (BAHIA, 2019f), em que foram reconhecidos 1,8 milhões de rostos, disparados 903 alertas e capturadas 44 pessoas com mandados de prisão ou foragidos.

O sistema disparou 903 alertas na Micareta de Feira de Santana em 2019, sendo cumpridos 18 mandados de prisão, mais a captura de 14 pessoas que descumpriam a prisão domiciliar (BAHIA, 2019f), fato destacado como eficiência da ferramenta, visto que seria muito difícil de poder ser repetido todas essas identificações e capturas por policiais em trabalho, a olho nu no universo de pessoas do evento.

Por outro lado, sob o aspecto do massivo reconhecimento de todas as pessoas que estavam na Micareta de Feira, em porcentagem, o uso do RF representou apenas 3,6% de veracidade dos alertas, o que poderia questionar a eficiência do sistema através de sua baixa acurácia nos alertas versus o direito à privacidade de todas as pessoas que foram reconhecidas (FALCÃO, 2021).

Para a fase do Projeto Vídeo Expansão, a partir de 2019, o objeto da licitação para aplicação de videomonitoramento e RF, via IA, mudou de instalação de câmeras e acessórios para a compra de serviços, o que seria uma vantagem, de forma que a vencedora da licitação Oi/Avantia, presta serviços de cessão e instalação dos equipamentos que permitem a operacionalização do videomonitoramento, suprindo a falta de profissionais da administração pública com especialização de tecnologias mais complexas, de ponta e ainda de prazos de

insumos, manutenções em equipamentos, através do exercício pelo servidor público de fiscalização da qualidade dos serviços prestados (BAHIA, 2019b).

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, resposta ao item 8 do questionário (2021), o que é considerado uma medida adotada de minimização de riscos de vazamento de dados pessoais sensíveis.

Uma forma de redução de riscos aos direitos fundamentais da liberdade, privacidade e proteção de dados pessoais que pode ser apresentada no Projeto Vídeo Expansão é a recomendação de abordagem das pessoas reconhecidas pelo algoritmo apenas com similaridade superior a 90% (BAHIA, 2019e), mesmo com a previsão do termo de referência – item 2.19.1.1.1 – que prevê a possibilidade de abordagem a partir de 50% de similaridade e que merece ser destacada para efeitos da pesquisa, pois quanto mais alto o grau de similaridade, menores as chances de erros de reconhecimento pela ferramenta tecnológica provocando menos constrangimentos e privações ilegais de liberdade.

Cumpre observar outro mecanismo adotado pela SSP-BA de redução de riscos aos direitos fundamentais, acima mencionados, quanto a determinação no adendo II, item 1.3, do termo de referência da licitação do projeto Vídeo-Polícia Expansão, no sentindo de 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, 2019b).

Ainda um ponto positivo descoberto pela análise dos dados se referiu ao que, no Projeto de Vídeo Expansão, foi informado que mecanismos de participação popular foram utilizados na licitação para adoção do RF, a exemplo de audiência pública e documentos de avisos e resumos dos editais de publicação publicados no DOE e em jornais de grande circulação, conforme determina o artigo 54 da Lei de Licitações da Bahia, Lei nº 9.433/2005 – Resposta ao item 8 do questionário (2021).

A medida acima mencionada representou um avanço quanto a aplicação do princípio da publicidade previsto no artigo 37 da CF e prestação de contas – *acountabillity*, diferentemente do que ocorreu em 2018, com o RF instituído por aditivo e sem mecanismos de participação popular e publicidade legal.

Há destaque para o fato da licitação do Projeto Vídeo-Polícia Expansão também ter sido supervisionada pelo Ministério Público, TCE-BA e da PGE-BA (BAHIA, 2021a), 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, no que tange aos dados coletados, quanto ao questionamento à SSP-BA de qual banco de dados é retirado as informações para a realização do RF, a pesquisa encontrou dissonância de respostas. A resposta da ASTEC/SSP-BA ao item 4 do questionário (2021), afirma que o banco de dados de mandados de prisão e desaparecidos é de fonte exclusiva da SSP-BA e alimentada por esta.

Já em entrevista ao repórter Salviano (G1, 2019) do programa Fantástico da TV Globo, o então Secretário de Segurança Pública da época informou que as redes sociais também seriam utilizadas como banco de dados para consulta pela SSP-BA, fato este que ficou comprovado na reportagem[15] e que pode ser assistida por completo no Quick Response Code (QR Code) (Figura 11), cujo manejo, basta apontar a câmera do seu celular para acesso ao link direto da reportagem.

Figura 11 – QR-Code – Reportagem do Fantástico em 2019

Fonte: G1 (2019).

Nesse esteio, há ainda a declaração do Coronel Marcos Oliveira ao site Intercept, de que a SSP-BA se utiliza das redes sociais com fonte aberta para fins específicos de investigação, sendo complementado pela assessoria de comunicação da SSP-BA de que essa prática era para localização de desaparecidos (FALCÃO, 2021) e uma resposta a LAI, em 2021, em que foi indicado pela SSP-BA também a consulta a Base Nacional de Mandados de Prisão do CNJ – BNMP 2.0 (PIRES et al, 2021).

A falta de entendimento e comunicação da SSP-BA quanto a qual base de dados utilizada para a prática do RF, se somente as oficiais em que a pessoa já tem um mandado de

[15] A reportagem completa do programa de televisão Fantástico sobre como as Câmeras de reconhecimento facial ajudam a polícia a encontrar criminosos realizada em 2019 também poderá ser acessada pelo endereço eletrônico disponível em: https://g1.globo.com/fantastico/noticia/2019/03/10/cameras-de-reconhecimento-facial-ajudam-a-policia-a-encontrar-criminosos.ghtml. Acesso em: 04/05/2021.

prisão em aberto ou está foragido ou desaparecido, ou quanto a possibilidade de uso de outros mecanismos de buscas, por exemplo, as redes sociais, pode representar para fins da pesquisa quanto ao uso indiscriminado da ferramenta tecnológica, sem transparência, prestação de contas, ou ainda proporcionalidade, na medida pelo reconhecimento de pessoas de forma indiscriminada, pode constituir uma possível sociedade da vigilância (HAN, 2018) instalada pelo Estado da Bahia.

A forma de operacionalização da ferramenta, sem transparência quanto à base de dados pelo Estado da Bahia, poderá impactar no 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 conferirá uma ilusão de liberdade social (NEGRI; OLIVEIRA; COSTA, 2020).

Mister esclarecer que, além do quanto afirmado anteriormente, ainda há a possibilidade do C*hilling Effect* (SOLOVE, 2011a) impactando no direito de liberdade de locomoção, expressão, associação que pode provocar inibição nas pessoas localizadas no Estado da Bahia quanto aos espaços públicos, o que confirmaria o argumento de Han (2018) quanto aos efeitos da vigilância massiva e de uma panoptismo digital e que poderia favorecer o controle e manipulação de massas, principalmente por governos autoritários e grandes empresas de tecnologia que detém o *know-how* da operacionalização da tecnologia.

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 (PNAD, 2018), por serem estes um público com maior incidência de erros de RF em pesquisas realizadas pelo mundo (BUOLAMWINI; GEBRU, 2018; NORRIS; ARMOSTRONG, 1999).

Importante observar que em pesquisa realizada pelo Observatório de Segurança Pública (2019), 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, segundo o Superintendente de Gestão Tecnológica e Organizacional da SSP-BA, Coronel PM Marcos Oliveira, que afirma que isso ocorreria apenas por uma consequência lógica da maioria da população da localidade que se autodeclarar preta ou parda (PALMA, PACHECO, 2020), o que diferiria da tese de racismo algoritmo, como defende Silva, T. (2021). .

Não foi possível averiguar na pesquisa o percentual exato de pessoas presas pelo uso do RF na Bahia que são pretos e pardos, porque os dados coletados se tratam de notícias que são divulgadas no site da SSP-BA e que nem todas as prisões têm fotos para comparação e análise da cor e raça das pessoas, o que poderá ser realizado em outros estudos.

Na análise dos dados, com base em respostas ao item 5 do questionário (2021), foi informado pela SSP-BA que, até novembro de 2021, não existiu erros no RF, por IA, tendo em vista o protocolo operacional utilizado pelas polícias para tal identificação que conduziram o capturado à prisão.

Ainda quando pesquisado na imprensa, em livros, artigos científicos e sites institucionais ou ainda notas oficiais governamentais sobre a existência de possíveis erros de prisão decorrentes de erro de identificação do RF, via IA, no Estado da Bahia que resultaram em prisões, não foi encontrado para fins desse trabalho indicações 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, houve o questionamento à SSP-BA e a resposta foi de que, até novembro de 2021, não havia conhecimento sobre erros de abordagem provocado pela indicação da ferramenta – Resposta ao item 7 do questionário (2021).

Cumpre destacar, entretanto, a existência de um possível erro de abordagem noticiado pelo Jornal Correio, ocorrida em 5 de janeiro de 2020, em que o RF errou ao identificar um assaltante procurado com um jovem negro de 25 anos e que tinha deficiência mental (PALMA; PACHECO, 2020), contudo, não foram encontrados em pesquisas realizadas pela autora um relatório com dados técnicos oficiais de quantidade de abordagens policiais por alertas do sistemas e o seu percentual de acertos e erros, inclusive na população negra, mulheres, transexuais, cisgêneros e não binários e que seriam o público mais propenso ao viés sexista algoritmo que se tornariam fatos importantes para a conclusão da pesquisa.

Destaca-se, entretanto, que, pela análise de percentual de abordagens de policiais no Brasil serem 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 a 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 algoritmo (SILVA, T., 2021), o que embasaria a manifestação pelo banimento do RF para fins de segurança pública na Bahia.

No que tange a possibilidade de compartilhamento dos dados biométricos com outros governos, empresas ou ainda mediante transferência internacionais, foi informado pela SSP-BA de 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 – Resposta ao item 9 do questionário (2021).

A justificativa apresentada foi a de que o armazenamento feito em *cloud* privada, através da instalação em *data center* da SSP-BA, possui acesso limitado, mediante autenticação ao ambiente e assinatura de termo de confidencialidade, tendo em vista que tais dados estão classificados na categoria de acesso restrito de sigilo – Resposta ao item 9 do questionário (2021), o que é um ponto positivo da aplicação da política.

Entretanto, o armazenamento físico no *data center* pode constituir-se de um risco físico de ataque de delinquentes, incêndio, ou outra causa que destrua os dados coletados ou sejam subtraídos no prédio onde fica localizado o centro de controle e que, inclusive, já é objeto de treinamento de segurança pelos novos policiais do Estado da Bahia na ACADELPOL (BAHIA, 2021c).

No que toca ao PRODETUR Salvador, apesar de ser um projeto de segurança turística do município de Salvador, ainda não em funcionamento, cuja operação das imagens será realizada pela guarda municipal, o fato de dispor de câmeras de RF a serem operadas pela SSP-BA faz com o projeto tenha que ser implementado de acordo com todas as observações das vantagens e riscos já avaliados no presente trabalho.

Importante trazer à baila que a utilização do RF pela segurança pública da Bahia é vista pela sociedade baiana de forma aceitável em sua maioria, visto que essa conclusão pode ser inferida no sentido de que há pouca oposição quanto a utilização do RF pela SSP-BA no poder judiciário ou ainda em notícias jornalísticas que versam sobre o tema.

Destacam-se dados consolidados no TJ-BA e instâncias superiores de 2018 até 2022, em que foi constatado apenas duas ações judiciais em que há o questionamento da legalidade do RF por IA, com resultado negativo para os autores e uma ação judicial do RF por videomonitoramento por CFTV, de resultado absolutório para o requerido, no universo de 282 prisões realizadas com a utilização da ferramenta até 30 de junho de 2022.

Observa-se que o Poder Judiciário da Bahia e o STJ, ainda em que pese serem apenas essas três ações, se posicionaram pela legalidade da aplicação do RF por IA como política pública, ainda que não haja regulação específica para utilização no Brasil.

8.5 CONSOLIDAÇÃO DA ANÁLISE DOS DADOS COLETADOS, DISCUSSÕES DOS RESULTADOS E APRESENTAÇÃO DE PROPOSIÇÕES DE MELHORIAS NA APLICAÇÃO DO RECONHECIMENTO FACIAL VIA INTELIGÊNCIA ARTIFICIAL PELA SECRETARIA DE SEGURANÇA PÚBLICA DA BAHIA

Para fins de consolidação da análise dos dados coletados para a pesquisa apresenta-se o Quadro 4, que sintetizará, de forma a contribuir para a compreensão sobre as vantagens, riscos e proposições de melhorias na aplicação da política pública investigada.

Quadro 4 – Vantagens, riscos e proposições de melhorias para aplicação do reconhecimento facial, via inteligência artificial como política de segurança pública no Estado da Bahia

Vantagens	**Riscos**	**Proposições de melhorias**
Política pública menos letal para os policiais e pessoas abordadas	Não há regulamentação legal específica sobre a aplicação da política de RF para a segurança pública na Bahia e aplicação inicial da política no Projeto Vídeo Policiamento – Mais Inteligência na Segurança e o PRODETUR Salvador não obtiveram participação popular, através de audiências públicas ou supervisão de órgãos de controle do Estado. Falta de transparência nos dados oficiais apresentados quanto à operacionalização da política pública e seus efetivos resultados.	Adotar o *Privacy By Design* nos projetos de implementação do RF como política pública e do Princípio da Precaução com preceitos éticos definidos e transparência; Adotar mecanismos de participação popular em debates sobre o tema e submissão a fiscalização de instituições de controle, como o Ministério Público, representantes da Sociedade Civil, TCE-BA e PGE-BA da Bahia; Construir Relatórios de Impacto a Proteção de Dados (RIPD). Implementar ações que venham a ser indicadas no Relatório da Comissão de Juristas do Senado Federal responsável por minutar o esboço de lei de regulamentação da IA no Brasil e que se apliquem diretamente à segurança pública.
Identificação e Captura de 282 pessoas de 2018 a 30 de junho de 2002 e redução de crimes contra a propriedade durante a aplicação da política de RF no Estado da Bahia, após a sua implantação.	Estímulo a associação de segurança ao encarceramento.	Realizar ações preventivas de educação para a sociedade civil e de inteligência para as polícias, visando a redução da prática dos crimes e, posteriormente, que permitam a ressocialização dos presos.
Investimento de recurso financeiros na segurança pública com custo-benefício.	Utilização indevida de recurso públicos com valores vultosos que somados chegaram a mais de R$ 600 milhões de reais.	Promover o acesso à fiscalização pelos órgãos de controle e realização de prestação de contas – *acoutabillity* – e transparência dos recursos investidos.
Reconhecimento de pessoas e análise se são foragidos da justiça ou desaparecidos. Ainda adoção de reconhecimento de placas de carros com sistemas que levam até um	Risco de ampliação do RF de milhares de pessoas, tratando-as de forma geral como suspeitas, quando o RF deveria ser adstrito	Adotar mecanismos de controle de acesso, definição da finalidade, necessidade e proporcionalidade do RF das pessoas.

Vantagens	Riscos	Proposições de melhorias
minuto mediante recursos tecnológicos com mobilidade, a exemplo de informações em tempo real em tablets e celulares na equipe de policiais que estão na rua.	aos objetivos e finalidades previamente dispostas. Ainda há risco de utilização dos dados biométricos captados de forma indiscriminada por governos autoritários para manipulação das massas com fins políticos ou pessoais.	Adotar tempo máximo de monitoramento contínuo pelo RF. Analisar e cadastrar apenas dados pessoais biométricos das pessoas que tiveram seu reconhecimento de acordo com as bases de dados dos foragidos, desaparecidos e com mandados de prisão em aberto e não de todas as pessoas que passaram pelo RF (Princípio da minimização dos dados).
Interoperabilidade de sistemas e banco de dados nacional de foragidos e procurados pela justiça.	Verificação operacional dos acessos para concessão de controles, visando prevenir incidentes de vazamentos de dados pessoais sensíveis na interoperabilidade dos sistemas.	Adotar controles de acesso mediante senhas fortes e com trocas periódicas e ainda outras ações e técnicas de segurança da informação.
Adoção de novos modelos de gestão, utilização de mão de obra especializada em tecnologias mais complexas, prazos de insumos, reposição de peças, conservação de ativos de forma mais célere. Exercício dos servidores públicos como fiscal de qualidade e prestabilidade dos serviços.	Há o risco de concessão de acessos indevidos aos bancos de dados biométricos da SSP-BA pelos terceirizados que prestarão os serviços de operacionalização do sistema.	Adotar sistemas rígidos de investigação sobre possível responsabilidade por acessos não autorizados e incidentes de vazamento tantos dos terceirizados quanto dos servidores públicos responsáveis pela fiscalização.
Cloud privada para armazenamento de dados no *data center*.	Risco físico de danos à estrutura do CIGE ocasionando destruição, manipulação indevida ou roubo da base de dados sensíveis.	Adotar treinamento pelas polícias quanto a prevenção de incidentes e riscos físicos de danos ao prédio do *data center* e realização de backups em servidores em *cloud* privada.
Realização de controle de acesso e classificação dos dados biométricos coletados pelo RF como sigilosos e acessos restritos.	Vazamento de senhas de acesso, hackeamento da base de dados.	Adotar o princípio da minimização dos dados e treinamentos de segurança de informação para os servidores públicos com acesso aos dados biométricos coletados e pseudoanimonização.
Melhorias e efetividade logística na mobilização de equipes de policiais para acesso dos alertas do RF.	Há riscos de mobilização de equipes de policiais para abordagem de pessoas, cujo alerta do RF não restou comprovado, ocasionado dispêndio de recursos e tempo, provocando atrasos em detrimento de um chamado de uma ocorrência real.	Realizar treinamentos e protocolos bem definidos de abordagem das pessoas supostamente reconhecidas pelo RF de forma a proporcionar segurança ao policial e à pessoa que será abordada evitando constrangimentos e ações contundentes de violência.
Adoção de abordagem com mais de 90% de similaridade.	Risco de que mesmo o percentual ser maior que 90% ainda gerar abordagens e constrangimento de pessoas indevidamente reconhecidas pela ferramenta.	Proporcionar um *double check* no RF pela tecnologia e por um agente do Estado antes da abordagem as pessoas reconhecidas.
Não compartilhamento de informações e dados sensíveis	A adoção do não compartilhamento minimiza os	Estabelecer protocolos de segurança da informação e

Vantagens	Riscos	Proposições de melhorias
coletados com as empresas de tecnologia que fornecem os serviços e outros países internacionais.	riscos de incidentes de vazamentos de dados pessoais e utilização indevida destes.	definição de uma política de não compartilhamento de dados ou ainda, de responsabilização por acesso indevido.
No Projeto Vídeo-Polícia Expansão há previsão de não realização de análise comportamental ou situacional por RF.	A adoção desse procedimento minimiza os riscos de violação à privacidade e proteção de dados pessoais.	Que seja definida e aplicada em lei futura específica a não possibilidade de utilização do RF para ações invasivas à privacidade e proteção de dados, como a análise situacional e comportamental das pessoas, ou ainda no âmbito estadual nos termos de referência das licitações vinculativos ao Edital.
Projeto Vídeo-Polícia Expansão com adoção de mecanismos de participação popular, tais como audiência pública, além da supervisão da licitação pelo TCE-BA, Ministério Público e PGE- BA	Os mecanismos de participação popular e supervisão de instituições de fiscalização minimizam riscos do projeto Vídeo-Polícia Expansão, mas destaca que estas medidas não foram utilizadas no projeto inicial Vídeo-Polícia: Mais Inteligência na Segurança e que podem gerar futuras impugnações.	Instituir órgãos de controle quanto à verificação prévia da necessidade, proporcionalidade e finalidade da utilização da RF, evitando excessos e ações indiscriminadas sobre as pessoas.
Não há existência de erros de prisões realizadas pelo RF na Bahia.	Um dado positivo de inexistência de prisões por erro de reconhecimento na Bahia, contudo, por ser uma tecnologia em que há possibilidade de erros de acurácia e vieses raciais e sexistas, os erros podem acontecer e violar o direito fundamental de liberdade das pessoas indevidamente reconhecidas e presas.	Realizar pesquisas e relatórios técnicos em que sejam apresentadas ao público não apenas os erros de prisões se utilizando do RF, mas também uma estimativa de quantas abordagens realizadas pelos alertas da ferramenta foram procedentes. Avaliar a contratação de ferramentas de RF em que sejam comprovados a constituição de uma base diversificada de raça e gênero na construção do algoritmo.
Apoio popular na Bahia quanto a adoção do RF e pouco questionamento judicial das prisões relacionadas com reconhecimento da ferramenta.	O risco se refere à mudança da opinião pública quanto à adoção da política e ao ajuizamento de diversas ações judiciais com questionamento legais de sua aplicabilidade do RF na segurança pública e *Chilling Effect*.	Adotar mecanismos de permitir o exercício aos direitos dos titulares dos dados pessoais quanto à confirmação, acesso e até correção de seus dados pessoais de posse da segurança pública (artigo 18 – LGPD). Publicizar a localização das áreas monitoradas pelas câmeras de RF com avisos de monitoramento.
Adoção de posicionamentos favoráveis no poder judiciário baiano e STJ sobre a aplicação da política pública.	Mudança de entendimento das cortes superiores quanto a ilegalidade da política, que se adotada repercussão geral no STF poderá anular todas as prisões realizadas com o uso da ferramenta até a data da decisão.	Mobilizar a sociedade civil e do próprio Estado da Bahia para regulamentação legal da política pública de RF na segurança evitando conflitos e alegação de supostas e inconstitucionalidades e ilegalidades no poder judiciário.

Fonte: Elaborado pela autora (2022).

Por fim, entende-se pela análise e discussões dos dados coletados de que houve a confirmação do pressuposto do trabalho de que há necessidade de mais acuidade na aplicação do RF pelo Estado da Bahia para utilização do RF como política pública de segurança, a fim de evitar possíveis violações de direitos fundamentais das pessoas, da liberdade, privacidade e proteção de dados pessoas.

Dessa maneira, recomenda-se que deve ser aplicado de imediato as proposições de melhorias, respeitados os direitos fundamentais da liberdade, privacidade e proteção de dados pessoais e os princípios da LGPD que se apliquem à administração pública e que não conflitem com as atribuições e resguardos da segurança pública, até que se tenha uma legislação específica sobre essa política pública.

9 CONSIDERAÇÕES FINAIS

Um tema instigante que denotou interdisciplinaridade ao tratar sobre ações de governança, direito e políticas públicas na sociedade contemporânea. O presente trabalho constitui-se de análises, caracterizações e proposições de melhorias quando do seu estudo sobre a política de segurança pública por videomonitoramento, via IA, aplicada pela SSP-BA.

Iniciou-se a pesquisa em busca da resposta para a seguinte pergunta: quais os benefícios e desafios da utilização da tecnologia de 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?

Nesse esteio, apresentou como objetivo geral, analisar os principais benefícios e riscos da implementação da acima referida política pública, visando apresentar e discutir os projetos Vídeo Policiamento – Mais Inteligência na Segurança; Vídeo-Polícia Expansão e PRODETUR Salvador.

Ainda, no que tange aos objetivos específicos do estudo, buscou-se descrever a evolução da sociedade e o impacto das TICs, mediante um breve relato histórico que perpassou pelo impacto das revoluções industriais, surgimento da Sociedade da Informação e evolução para o desenvolvimento do Panoptismo Digital.

Nesse diapasão, destacaram-se o fato de que o impacto das TICs e o surgimento da internet, principalmente após 1987, com a internet comercial, contribuíram de sobremaneira, para a valorização da informação e, posteriormente, do tratamento de dados pessoais como um ativo extremamente valioso para a construção de perfis de consumo, difundir produtos e serviços e proporcionar mais lucros e riquezas para as empresas que detém o know-how da tecnologia e controle e poder para os governos.

A construção de perfis das pessoas, através da exploração do corpo humano, em sua forma de extração de dados biométricos e análise comportamental ou de emoções para personalizar seus produtos e serviços, levou-se a conclusão de que esta prática, se realizada de forma reiterada e indiscriminada poderia implicar, caso não haja controle efetivo desta utilização, em uma sociedade da vigilância, marcada pelo panoptismo digital.

No que tange a aplicação da tecnologia de IA de RF como política pública no Brasil, buscou-se caracterizar quais seriam essas políticas, identificando planos ou projetos no Brasil, a partir da aplicação das tecnologias de IA.

Observou-se a temporalidade, a partir dos anos 2000, do estímulo à formulação de políticas públicas envolvendo a tecnologia (BRASIL, 2000) e a primeira menção ao RF, via IA,

no PNSP 2018-2028 para fiscalização de fronteiras, portos e aeroportos. Pelo estudo, foi constatado de que houve uma maior formulação de políticas públicas de natureza tecnológica, principalmente após a existência de editais de financiadoras públicas, a partir de 2012.

Desta feita, uma vez identificada as políticas públicas utilizando-se da tecnologia de IA, especialmente o RF na segurança pública, importante se mostrou analisar a utilização – contribuições e limites – da RF, sob a ótica dos direitos fundamentais da liberdade, privacidade e proteção dos dados pessoais.

A análise acima mencionada demonstrou que os principais benefícios estão circunscritos à utilização do videomonitoramento com uma política pública menos letal que se utiliza da tecnologia de forma mais assertiva e permite que as polícias possam planejar as ações com mais inteligência e atendimento ao princípio da universalidade e eficiência.

Outros pontos positivos encontrados foram: a utilização de softwares muito rápidos na comparação de imagens e que permitem flexibilidade e mobilidade das equipes policiais na atuação preventiva de crimes e na captura de pessoas foragidas ou com mandados de prisão em aberto; a possibilidade das imagens poderem ser utilizadas nos processos como provas, redução de custos de pessoal e utilização de mão de obra qualificada para tecnologias mais complexas.

No que tange às limitações da tecnologia foram identificados erros do RF, por problemas de falta de acurácia dos softwares e a existência de vieses – histórico, representação e avaliação – com impactos raciais e sexistas nos algoritmos, que podem comprometer a confiabilidade da aplicação dessa tecnologia, aumentado o risco de violação a direitos fundamentais das pessoas, especialmente pelos critérios racial e de gênero.

Por outro lado, foi constatado que, com o avanço da tecnologia, as limitações técnicas dos softwares mais modernos estão em percentual de erros cada vez menores e que estudos como o de Buolanwini e Gebru (2018) demostram a possibilidade de correção de vieses nos algoritmos de IA que compõe as bases de dados de análise do RF, o que pode ser realizado, dentre outras formas, pela diversificação étnica da base de dados quando da construção do algoritmo.

Diante da possibilidade de possíveis erros e vieses algoritmos, o estudo partiu para uma análise quanto a existência de regulamentação legal específica para o uso da IA de RF na segurança pública no mundo e no Brasil sob o olhar dos direitos fundamentais da liberdade.

Concluiu-se que o uso indiscriminado do RF automatizado como política de segurança pública pode ocasionar violação ao direito constitucional e fundamental de liberdade e suas facetas – liberdade de expressão, locomoção, reunião e associação –, se houver monitoração eletrônica excessiva realizada pelo Estado e empresas de tecnologia, principalmente destacado

pela possibilidade dessa hipervigilância ser realizada por Estados totalitários e provocar a difusão do *Chilling Effect*.

Ainda, dentro da análise dos direitos fundamentais, no que tange às questões relativas à importância da proteção da privacidade na utilização da tecnologia de RF, destacam-se que, do mesmo modo, o monitoramento indiscriminado das pessoas na implementação da política pública multirreferenciada faz como que os indivíduos sempre sejam tratados como suspeitos.

A hipervigilância é nociva à democracia e não deve ser vista como normalizada e estimulada pelo Estado e grandes empresas de tecnologia, a fim de que não possa ser submergido o direito constitucional da privacidade, em face da difusão ilusória de que quem não deve não teme a supervigilância. Desta feita, o uso do RF como política pública não deve ser utilizado para a manipulação das massas com fins indiscriminados para que seja compatível com o exercício do direito à privacidade.

No que toca a proteção de dados pessoais, o estudo destaca, a importância desse direito ter sido previsto na CF como um direito fundamental, o que somente corroboraria a aplicação da LGPD à segurança pública via uma interpretação sistemática do artigo 4º e seus parágrafos.

Assim, para o presente trabalho defende-se a aplicação principiológica da LGPD na segurança pública, especificadamente quanto aos princípios da transparência, finalidade, necessidade, segurança da informação e não discriminação e ainda uma interpretação finalística da LGPD para defesa da aplicação à segurança pública dos conceitos de *Privacy by Design*, elaboração de RIPD e de alguns direitos dos titulares de dados pessoais, tais como: confirmação do tratamento, acesso aos dados e correção dos dados previstos no artigo 18, incisos I, II e III da referida lei – autodeterminação informativa.

No caso do Brasil, constata-se que não há lei especifica para a utilização do RF, via IA, na segurança pública, mas tão somente projetos de leis. Contudo há leis gerais que trazem princípios a serem respeitados para fins de utilização da internet e IA, como liberdade, privacidade e proteção de dados pessoais (LGPD, MCI, Lei da Inovação – Lei nº 10.973/2004) e Decreto nº 8.854/2019 que estabelece o Plano Nacional de Internet das Coisas (IOT)), e que poderiam ser aplicadas ao caso em tela.

Ainda foram encontrados na pesquisa a existência, no Brasil, de mais de 22 projetos de leis estaduais em tramitação que tentam regular o uso do RF, via IA, mas nenhum de forma completa, com destaque para o fato de que provavelmente esses projetos serão arquivados, em razão da inclusão em 2022 do inciso XXX, ao artigo 22 da CF que determinou que a competência para legislar sobre proteção de dados é privativa da União.

Assim, dentro da indefinição regulatória que acomete o Brasil sobre o tema, o fato é que há tentativa de regular a IA, mediante a criação da Comissão de Juristas pelo Senado Federal que poderá levar em consideração questões ligadas ao uso do RF na segurança pública, com ou sem dados pessoais, mas ainda não finalizada.

Durante o estudo constatam-se questões relevantes levantadas por entidades de direitos humanos e da sociedade civil, com destaque para pesquisadores do movimento negro, que promoveram campanhas a favor do banimento da referida tecnologia, pelos riscos de supressão da liberdade em população racializada, haja vista os vieses raciais e sexistas dos algoritmos.

Dentre os argumentos que embasaram a defesa do banimento, destacam-se a seletividade penal, falta de neutralidade da tecnologia, vigilância em espaços públicos de forma indiscriminada, inversão social do princípio da presunção da inocência, na medida em que se todos são vigiados, todos são considerados suspeitos.

Ainda, o estudo apresenta a existência de locais que já adotaram a recomendação do banimento da referida tecnologia, como São Francisco, Califórnia, EUA, e o parecer do EDPB e da EDPS que em junho de 2021 recomendaram o banimento desta em espaços públicos, por ser uma política pública de alto risco.

Quanto ao estudo de caso, especificamente, analisa-se os principais benefícios e riscos da implementação da multicitada política pública realizada pela SSP-BA, ainda em 2018, e apresenta-se, discute-se e propõe-se melhorias aos projetos Vídeo Policiamento – Mais Inteligência na Segurança, Vídeo-Polícia Expansão e PRODETUR Salvador.

Foram identificados pontos positivos nos projetos acima, no que tange a questões de eficiência e 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, das quais já totalizaram 282 pessoas foragidos e procurados pela justiça que foram capturadas pela ferramenta tecnológica até 30 de junho de 2022.

Além disso, outros pontos positivos também chamam atenção, tais como: o cumprimento dos direitos fundamentais, a exemplo da não utilização do RF para análise situacional ou comportamental das pessoas, previsto no adendo II ao Termo de Referência da Licitação do Projeto de Vídeo-Polícia Expansão; utilização no projeto 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; não compartilhamento de dados sensíveis biométricos com entidades privadas ou transferência internacional; existência de

controles de acesso aos dados; *cloud* 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 no questionário quanto a existência de protocolo interno nas polícias da Bahia relativos à abordagem das pessoas, possivelmente reconhecidas pelo RF, para apenas se tiverem sido apontadas pela tecnologia com similaridades acima de 90%, o que reduziria chances de erros no RF, quando há no Termo de Referência da licitação do projeto Vídeo-Polícia Expansão, a possibilidade da abordagem já poder ser realizada acima de 50%.

Por outro lado, identificam-se riscos aos direitos fundamentais da liberdade, privacidade e proteção de dados pessoais quando da operacionalização da multirreferida política, com destaque para a falta de uma regulamentação legal específica e 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 realizados previamente audiências públicas e debates com a sociedade civil e órgãos de controle do Estado quanto a 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 direito fundamentais das pessoas.

Dentro dos dados coletados, conclui-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 quanto a respostas a 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.

Assim, se a consulta para o RF for dos bancos de dados dos foragidos e desaparecidos da própria SSP-BA ou com interoperabilidade com o BNMP 2.0 do CNJ há uma finalidade e proporcionalidade da medida, visto que a finalidade é a captura de foragidos e com mandados de prisão em aberto, todavia, uma vez que redes sociais/mecanismos de busca, forem utilizadas de forma geral, a política poderá será utilizada de forma indiscriminada, violando a privacidade e proteção de dados pessoais que não se aplicariam ao perfil de aplicação da política e não

haveriam necessidade de terem seus dados biométricos colhidos pelo sistema e armazenados e tratados pela SSP-BA, correndo ainda o risco de utilização desses dados para manipulação das massas e uso político ou para fins pessoais para controlar cidadãos.

Conclui-se, portanto, que a ampliação da base de dados para as redes sociais ou internet em geral somente se permitiria com mitigação para a tentativa de localização de pessoas desaparecidas.

Por fim, ressalta-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 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 em violação ao princípio de minimização previsto na LGPD.

A partir das análises realizadas, propõe-se melhorias na implementação da política pública, recomendando a observância dos princípios constitucionais da liberdade, privacidade e proteção de dados pessoais, de forma que esta seja planejada e executada com *Privacy by Desing*, transparência, conceitos éticos, limites, finalidade específica, prestação de contas – *acontabillity*, proporcionalidade e não discriminação.

E as proposições de melhoria continuam de forma a recomendar a previsão de planos de incidentes de vazamento de dados, RIPD e relatórios técnicos periódicos que apresentem mais dados sobre os resultados da política ao público, de forma a contemplar, por exemplo, a quantidade de abordagens policiais que incorreram por alertas falsos da ferramenta.

Sugere-se a adoção da aplicação da minimização dos dados armazenados, pseudoanonimização, trocas de senhas de acesso periódicas do sistema e ainda adoção de canal para exercício dos direitos dos titulares dos dados pessoais ao acesso, confirmação e correção de seus dados e tempo máximo de monitoramento contínuo.

Recomenda-se um *double check* no RF pela tecnologia e por um agente do Estado, antes da abordagem às pessoas reconhecidas, e a adoção de ações educativas e treinamentos para os policiais, a fim de evitar a abordagem violenta como regra.

Ainda, propõe-se como melhorias a promoção do envolvimento da sociedade civil, proporcionando mais debates sobre a política com participação de órgãos de controle e estabelecimento de protocolos de segurança da informação e responsabilização por infração para os servidores públicos ou terceirizados que descumpram as normas legais, respeitado os princípios do processo administrativo e ampla defesa e o contraditório.

No campo da contestação judicial da política em tela, traz-se à baila a conclusão de que as ações judiciais que foram levadas ao TJ-BA e ao STJ, e que questionaram a utilização da multirreferida política pública foram julgadas favoráveis ao Estado da Bahia.

Contudo, como o universo das ações judiciais em curso foram de apenas três e não há jurisprudência consolidada sobre o assunto e nem regulamentação legal específica, o estudo chama a atenção para o fato de que se houver mudança de entendimento do Poder Judiciário quanto a legalidade de aplicação da política pública de RF no Estado da Bahia, isso poderá implicar na anulação de todas as prisões realizadas com base no RF feito pela ferramenta tecnológica, se for declarada efeitos retroativos – *ex tunc* – à data da decisão judicial.

Dessa maneira, a pesquisa reconhece que há benefícios e desafios na aplicação do RF, por IA, como política pública e por isso propõe melhorias para sua utilização, de forma a minimizar os riscos de violação aos direitos fundamentais da liberdade, privacidade e proteção de dados pessoais.

O entendimento acima também leva em consideração que já foram investidos mais de R$ 665 milhões na implementação da multicitada política pelo Estado da Bahia e até a entrega da pesquisa não houve informações quanto a erros na ferramenta que implicaram em privação de liberdade indevida das pessoas.

Dessa forma, conclui-se quanto a possibilidade de uma regulação legal específica constituir na compatibilização da política com os direitos fundamentais da liberdade, privacidade e proteção de dados pessoais na aplicação da multicitada política de RF na segurança pública do Estado da Bahia.

Quando da realização da pesquisa, ressalta-se algumas limitações, a exemplo de escassez de divulgação de dados institucionais oficiais, por ser uma política pública recente e por questões relativas à segurança pública sofrerem restrições de confidencialidade e sigilo. Além disso, também não foi esgotada análise sobre todas as leis e políticas dos países indicados na pesquisa como comparativos para o trabalho.

Outro fator limitador à pesquisa é a pandemia de Covid-19 e a declaração de emergência pública sanitária, a partir de 2020, que impactou deveras a sociedade em todo o mundo, cujo isolamento social provocou o fechamento de comércios, suspensão de aulas presenciais em todos os níveis escolares, inclusive com fechamento de bibliotecas físicas, restringindo o acesso a um acervo teórico mais amplo.

Diante dos resultados apresentados pela pesquisa, , espera-se abrir oportunidades para estudos posteriores, principalmente, pela complexidade e sensibilidade do tema que envolve

políticas públicas de segurança, eficiência operacional, inovação e direitos fundamentais da liberdade, privacidade e proteção de dados pessoais.

Destaca-se que há previsão para dezembro de 2022 da apresentação do Relatório da Comissão de Juristas do Senado Federal que regulará a Inteligência Artificial no Brasil e que poderá trazer conclusões que impactam totalmente na aplicação da política pública de reconhecimento facial automatizado pelo Estado da Bahia, seja em sua regulação, moratória ou até banimento e poderá embasar outros estudos sobre o tema.

REFERÊNCIAS

ADA LOVELACE INSTITUTE. **Beyond face value**: public atitudes to facial recognition technology. London, sept. 2019. Disponível em: https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf. Acesso em: 04 mar. 2022.

AGRAWAL, A.; GANS, J.; GOLDFARB, A. Economic Policy for Artificial Intelligence. **Innovation Policy and the Economy**, v. 19, n. 1, p. 139-159, 2019.

ALBARDEIRO, N. M. E. **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, 2020. 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.; BUENO, S.; LIMA, R. S. de. Evolução das mortes violentas intencionais no Brasil. **Anuário Brasileiro de Segurança Pública 2021**, [São Paulo], ano15, 2021. ISSN 1983-7364. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2021/07/anuario-2021-completo-v4-bx.pdf. Acesso em: 03 maio 2022

ALCADIPANI, R. Novas tecnologias e a criminalidade: o crime do futuro e a polícia do passado. **Estadão**, São Paulo, 14 jan. 2020. 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.; PACHECO, D. Negro correndo é ladrão? **Folha de São Paulo**, São Paulo, 11 nov. 2020. Disponível em: https://piaui.folha.uol.com.br/negro-correndo-e-ladrao/. Acesso em: 04 mar. 2022.

ALMEIDA, E. C. Os grandes irmãos: o uso da tecnologia de reconhecimento facial para a persecução penal. **Revista Brasileira de Segurança Pública**, São Paulo, v. 16, n. 2, p. 264-283, fev.-mar. 2022. Disponível em: https://revista.forumseguranca.org.br/index.php/rbsp/article/view/1377/548. Acesso em: 04 jun. 2022.

ALVES, I. S. **Reconhecimento Facial no auxílio à segurança pública da cidade de Florianópolis**. 54 f. 2020. TCC (Especialização) – Universidade do Sul de Santa Catarina. Florianópolis, 2020. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/11998. Acesso em: 06 jan. 2022.

ALVES, S. **Além do racismo, reconhecimento facial erra mais em pessoas trans**. Uol, São Paulo, 14 fev. 2021a. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/02/14/nao-e-so-racismo-reconhecimento-facial-tambem-erra-mais-em-pessoas-trans.htm. Acesso em: 04 out. 2021.

ALVES, S. **Pelourinho vai ganhar câmeras de reconhecimento facial:** isso é bom ou ruim? Uol, São Paulo, 01 mar. 2021b. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/03/01/pelourinho-vai-ganhar-cameras-de-reconhecimento-facial-isso-e-bom-ou-ruim.htm. Acesso em: 05 jun. 2022.

ALSUR. **Reconhecimento facial na América Latina: t**endências na implementação de uma tecnologia perversa. 2021. Disponível em: https://www.alsur.lat/pt-br/relatorio/reconhecimento-facial-na-america-latina-tendencias-na-implementacao-uma-tecnologia. Acesso em: 29 jan. 2022.

AMAZONAS. (Estado). Secretaria de Segurança Pública. **Retrato Falado:** procedimento que auxilia a polícia na elucidação de crimes. Manaus, 2020. Disponível em: http://www.ssp.am.gov.br/retrato-falado-procedimento-auxilia-policia-na-elucidacao-de-crimes/. Acesso em: 30 mar. 2022.

AMAZON. **We are implementing a one-year moratorium on police use of Rekognition**. [s.l.], jun. 10, 2020a. Disponível em: https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition. Acesso em: 01 fev. 2022.

_____. **What is Amazon Rekognition?** [s.l.], 2020b. Disponível em: https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html. Acesso em: 01 fev. 2022.

ANDRADE, M. **SSP recebe Prêmio Case de Sucesso com Reconhecimento Facial**. Salvador: Secretaria de Segurança Pública. Salvador, 17 set. 2019. Disponível em: http://www.ssp.ba.gov.br/2019/09/6446/SSP-recebe-Premio-Case-de-Sucesso-com-Reconhecimento-Facial.html. Acesso em: 31 maio 2021.

AQUALTUNELAB. **Documento preto I**: Contribuições do Aqualtune Lab para o debate sobre regulação da Inteligência Artificial no Brasil. São Paulo, maio 2022. Disponível em: https://www.aqualtunelab.com.br/wp-content/uploads/2022/06/AQUALTUNELAB-DocumentoPreto-AI-V1-digital.pdf. Acesso em: 03 jun. 2022.

ARANHA, E.; FERREIRA, L. M. T. **O direito fundamental à proteção de dados e a importância da proposta de alteração constitucional nº 17/2019**. Rio de Janeiro: OAB-RJ, 27 jan. 2020. Disponível em: https://www.oabrj.org.br/noticias/artigo-direito-fundamental-protecao-dados-importancia-proposta-alteracao-constitucional. Acesso em: 22 jul. 2021.

ARAS, J. PONTES, Mayanne; FIGUEIREDO, Pedro Camilo (org.). **A aplicabilidade da Lei Geral de Proteção de Dados à Administração Pública. Lei Geral de Proteção de Dados. Novos paradigmas do direito do Brasil**. Salvador: Mente Aberta, jun. 2020.

ARAUJO, R. A.; CARDOSO, N. D.; PAULA, A. M. Regulação e uso do Reconhecimento facial na Segurança Pública do Brasil. **Revista de Doutrina Jurídica**, Brasília-DF, v. 112, 2021.

AUGUSTO, T. **Há 26 anos, WWW em domínio público permitiu a expansão da Internet como conhecemos**. abr. 2019. Disponível em: https://canaltech.com.br/internet/ha-26-anos-

www-em-dominio-publico-permitiu-expansao-da-internet-como-conhecemos-138027/. Acesso em: 04 jun. 2021.

BAHIA. **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. Salvador, 2016a. Disponível em: http://www.legislabahia.ba.gov.br/documentos/decreto-no-16852-de-14-de-julho-de-2016. Acesso em: 12 maio 2022.

_____. **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 de Segurança Pública. Leis estaduais, [s.l.], 2016b. Disponível em: https://leisestaduais.com.br/ba/decreto-n-16852-2016-bahia-institui-o-centro-de-operacoes-e-inteligencia-e-o-comite-de-gestao-de-crises-no-ambito-da-secretaria-da-seguranca-publica. Acesso em: 03 jun. 2021.

_____. Decreto nº 21.235, de 09 de março de 2022. Institui o projeto Câmera Interativa e dá outras providências. **Diário Oficial do Estado**, Salvador, 2022a. Disponível em: https://www.ssp.ba.gov.br/arquivos/File/Camera/DECRETO.pdf. Acesso em: 14 maio 2022.

_____. **Governo institui projeto que permite uso de câmeras privadas para investigar crimes**. 10 mar. 2022b. Disponível em: https://bahia.ba/bahia/governo-institui-projeto-que-permite-uso-de-cameras-privadas-para-investigar-crimes/.Acesso em: 15 jun. 2022.

_____. Secretaria de Comunicação Social. **Governo da Bahia contrata empresa que vai disponibilizar o sistema do Projeto Vídeo-Polícia**. Salvador, 20 maio 2022c. Disponível em: https://www.bahia.ba.gov.br/2022/05/area-de-imprensa/governo-da-bahia-contrata-empresa-que-vai-disponibilizar-o-sistema-do-projeto-video-policia-2/. Acesso em: 15 jun. 2022.

_____. Secretaria de Comunicação Social. **Parque tecnológico está com editais abertos para atrair novas startups e empresas residentes**. Salvador, 16 dez. 2020a. Disponível em: https://www.bahia.ba.gov.br/2020/12/noticias/inovacao/parque-tecnologico-esta-com-editais-abertos-para-atrair-novas-startups-e-empresas-residentes/.Acesso em: 15 jun. 2022.

_____. Secretaria de Segurança Pública. **Bahia alcança quase 26% de redução em roubos de bancos**. Salvador, 13 jan. 2020b. Disponível em: https://www.ssp.ba.gov.br/2020/01/7052/Bahia-alcanca-reducao-de-quase-26-em-roubos-a-bancos.html. Acesso em: 24 ago. 2021.

_____. Secretaria de Segurança Pública. **Bahia apresenta resultado do reconhecimento Facial na China**. Salvador, 14 maio 2019a. Disponível em: https://www.ssp.ba.gov.br/2019/05/5695/Bahia-apresenta-resultado-do-Reconhecimento-Facial-na-China.html. Acesso em: 03 abr. 2021.

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

BAHIA. Secretaria de Segurança Pública da Bahia. **Projeto Básico de Monitoramento Eletrônico por Câmeras em Vias Públicas, para a Cidade de Salvador da Superintendência de Inteligência - SI**. Salvador, 2009.

_____. Secretaria de Segurança Pública. **DPT realiza identificação humana de foragidos através do celular**. Salvador, 24 fev. 2020c. Disponível em: https://www.ssp.ba.gov.br/2020/02/7282/DPT-realiza-identificacao-humana-de-foragidos-atraves-de-celular.html. Acesso em: 24 ago. 2021.

_____. Secretaria de Segurança Pública. **Em duas horas assaltantes são achados com auxílio de tecnologia**. Salvador 31 maio 2022d. Disponível em: https://www.ssp.ba.gov.br/2022/05/12347/Em-duas-horas-assaltantes-sao-achados-com-auxilio-de-tecnologia.html. Acesso em: 30 maio 2022.

_____. Secretaria de Segurança Pública. **Em quatro dias 6,5 milhões pessoas passaram pelos portais**. Salvador, 24 fev. 2020d. Disponível em: http://www.ssp.ba.gov.br/2020/02/7283/Em-quatro-dias-65-milhoes-de-pessoas-passaram-pelos-portais.html. Acesso em: 24 ago. 2021.

_____. Secretaria de Segurança Pública. **Governador autoriza expansão de tecnologia a mais 77 cidades baianas**. Salvador, 27 jul. 2021a. 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.

_____. Secretaria de Segurança Pública. **Histórico CIGE**. Salvador, 2013. Disponível em: https://www.ssp.ba.gov.br/modules/conteudo/conteudo.php?conteudo=25. Acesso em: 05 maio 2022.

_____. Secretaria de Segurança Pública. **Ordem de serviço ampliará Reconhecimento e de Placas**. Salvador, 26 jul. 2021b. Disponível em: https://www.ssp.ba.gov.br/2021/07/10135/Ordem-de-servico-ampliara-Reconhecimento-Facial-e-de-Placas.html. Acesso em: 01 abr. 2021.

_____. Secretaria de Segurança Pública. Portaria nº 107, de 30 de março de 2022. Regulamenta o mecanismo de adesão dos interessados em participar do Projeto Câmera Interativa. **Diário Oficial do Estado**, Salvador, 2022e.

_____. Secretaria de Segurança Pública. **Procurados por roubo lideram lista de prisões com auxílio de tecnologia**. Salvador, 26 jan. 2022f. Disponível em: http://www.ssp.ba.gov.br/2022/01/11492/Procurados-por-roubo-lideram-lista-de-prisoes-com-auxilio-de-tecnologia.html. Acesso em: 05 abr. 2022.

_____. Secretaria de Segurança Pública. **Reconhecimento facial bate recorde com 11 encontrados em 24h**. Salvador, 29 jun. 2022g. https://www.ssp.ba.gov.br/2022/06/12555/Reconhecimento-Facial-bate-recorde-com-11-encontrados-em-24h.html. Acesso em: 14 jul. 2022.

_____. Secretaria de Segurança Pública. **Reconhecimento facial completa um ano e é destaque nacional**. Salvador, 18 dez. 2019b. Disponível em:

http://www.ssp.ba.gov.br/2019/12/6981/Reconhecimento-Facial-completa-um-ano-e-e-destaque-nacional.html. Acesso em: 24 ago. 2021. Era f.

_____. Secretaria de Segurança Pública. **Reconhecimento Facial é destaque no primeiro semestre**. Salvador, 09 ago. 2019c. Disponível em: http://www.ssp.ba.gov.br/2019/08/6179/Reconhecimento-Facial-e-destaque-no-primeiro-semestre-.html. Acesso em: 24 ago. 2021.

_____. Secretaria de Segurança Pública. **Reconhecimento Facial estará nos portais e em outros locais**. Salvador, 26 fev. 2019d. 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.

_____. Secretaria de Segurança Pública. **Reconhecimento Facial flagra foragido usando máscara**. Salvador, 01 set. 2020e. Disponível em: http://www.ssp.ba.gov.br/2020/09/8319/Reconhecimento-Facial-flagra-foragido-usando-mascara.html. Acesso em: 01 set. 2021.

_____. Secretaria de Segurança Pública. **Reconhecimento facial impede entrada de homicida em circuito**. Salvador, 05 mar. 2019e. 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.

_____. Secretaria de Segurança Pública. **Reconhecimento facial resulta nas prisões de 33 pessoas**. Salvador, 2019f. Disponível em: http://www.ssp.ba.gov.br/2019/04/5613/Reconhecimento-Facial-resulta-nas-prisoes-de-33-pessoas.htm. Acesso em: 03 abr. 2021.

_____. Secretaria de Segurança Pública. **SSP dá início a operação de 1200 câmeras inteligentes**. 13 jun. Salvador, 2022h. Disponível em: https://www.ssp.ba.gov.br/2022/06/12455/SSP-da-inicio-a-operacao-de-1200-cameras-inteligentes.html. Acesso em: 04 fev. 2022.

_____. Secretaria de Segurança Pública. **SSP recebe Prêmio Case de Sucesso com Reconhecimento facial**. Salvador, 17 set. 2019g. https://www.ssp.ba.gov.br/2019/09/6446/SSP-recebe-Premio-Case-de-Sucesso-com-Reconhecimento-Facial.html. Acesso em: 03 abri. 2021.

_____. Secretaria de Segurança Pública. **Tecnologia e Contrainteligência são temas de instrução**. Salvador, 15 dez. 2021c. Disponível em: https://www.ssp.ba.gov.br/2021/12/11239/Tecnologia-e-contrainteligencia-sao-temas-de-instrucao.html. Acesso em: 03 fev. 2022.

_____. Secretaria de Segurança Pública. **Termo de Referência Projeto Vídeo Polícia Expansão**. Salvador, 2019h. Disponível em: https://comprasnet.ba.gov.br/sites/default/files/termo_de_referencia_v1.pdf. Acesso em: 02 set. 2021.

BAHIA. Tribunal de Justiça do Estado da Bahia. **Lançado sistema de videomonitoramento inteligente de segurança**. Salvador, 2018. Disponível em: http://www5.tjba.jus.br/portal/jurisprudencia/. Acesso em: 16 jun. 2022.

BARBOSA, Attila Magno e Silva. **Da disciplina ao controle**: novos processos de subjetivação no mundo do trabalho. Disponível em: https://periodicos.ufsc.br/index.php/politica/article/view/21757984.2012v11n22p75. Acesso em: 28 ago. 2013.

BARBOSA, Kátia Borges; SANTOS, Fabiele Almeida Dos. **Direitos humanos e segurança pública no Brasi**l: caminhos que se cruzam. Ceará: UECE, 2009.

BARIFOUSE, R. Por que 5G da Huawei põe Brasil em saia justa com China e os EUA. **BBC News Brasil**, São Paulo, 28 nov. 2019. Disponível em: https://www.bbc.com/portuguese/brasil-50468237. Acesso em: 02 set. 2020.

BARRETO FILHO, H. **Seis dos dez pré-candidatos ao governo de SP apoiam câmeras em fardas.** Uol, São Paulo, 08 maio 2022. Disponível em: https://www.uol.com.br/eleicoes/2022/05/08/candidatos-governo-sp-cameras-uniforme-pms.htm?cmpid=copiaecolahttps://www.uol.com.br/eleicoes/2022/05/08/candidatos-governo-sp-cameras-uniforme-pms.htm. Acesso em: 03 jun. 2022.

BATKINS, S. The Tech Giants Are Out to Get You. **Regulation**, v.52, p. 52-53, Summer 2019.

BAUMAN, Z. **Vigilância líquida:** diálogos com David, Lyon. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar, 2014.

BIG BROTHER WATCH. **Face Off:** the lawless growth of facial recognition in UK policing. [S.L.], may, 2018. Disponível em: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf. Acesso em: 5 maio 2020.

BIONI, B. R.; LUCIANO, M. O Princípio da Precaução na Regulação da Inteligência Artificial: seriam as leis de proteção de dados o seu portal de entrada? *In*: FRAZÃO, A.; MULHOLLAND, C. (org.). **Inteligência artificial e direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019.

BIONI, B. R. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2018.

BONAMIGO, I. S.; PEDRO, R. M. L. R.; MELGAÇO, L. **(In) Segurança Pública**: Cartografia de relações entre dispositivos de vigilância, políticas públicas e violências em espaços urbanos contemporâneos. Buenos Aires, 2016. Disponível em: https://lavits.org/wp-content/uploads/2017/08/P2_Salete_etal.pdf. Acesso em: 02 mar. 2022.

BLUM, R. O.; LOPEZ, N. LGPD no Setor Público. **Cadernos Jurídicos da Escola Paulista de Magistratura,** São Paulo, ano 21, n. 53, p. 171-177, jan.-mar. 2020.

BLUM, R. P. F. **O direito à privacidade e à proteção dos dados do consumidor**. São Paulo: Almedina, 2018.

BRASIL. Agência Brasileira de Inteligência. **ABIN apoia regulação de reconhecimento facial**. Brasília, DF, 05 abr. 2019a. Disponível em: https://www.gov.br/abin/pt-br/assuntos/noticias/abin-apoia-regulacao-de-reconhecimento-facial. Acesso em: 05 fev. 2022.

_____. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado, 1988.

_____. Lei nº 10.793, de 02 de dezembro de 2004. Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências. **Diário Oficial da União**, Brasília, DF, 03 dez. 2004. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/l10.973.htm. Acesso em: 04 ago. 2021.

_____. 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.

_____. Lei nº 12.403, de 04 de maio de 2011. Altera dispositivos do Decreto-Lei nº 3.689, de 3 de outubro de 1941 - Código de Processo Penal, relativos à prisão processual, fiança, liberdade provisória, demais medidas cautelares, e dá outras providências. **Diário Oficial da União**, Brasília, DF, 05 maio 2011a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12403.htm. Acesso em: 02 mar. 2021.

_____. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial da União**, Brasília, DF, 2011b.

_____. 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, DF, 29 jun. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12681.htm. Acesso em: 02 mar. 2021.

_____. 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. 2014a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 02 mar. 2021.

_____. Lei nº 13.675, de 11 de junho de 2018. Disciplina a organização e o funcionamento dos órgãos responsáveis pela segurança pública, nos termos do § 7º do art. 144 da Constituição Federal; cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS); institui o Sistema Único de Segurança Pública (Susp); altera a Lei Complementar nº 79, de 7 de janeiro de 1994, a Lei nº 10.201, de 14 de fevereiro de 2001, e a Lei nº 11.530, de 24 de outubro de 2007; e revoga dispositivos da Lei nº 12.681, de 4 de julho de 2012. **Diário Oficial da União**, Brasília, DF, 12 jun. 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13675.htm. Acesso em: 02 mar. 2021.

_____. 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. 2018b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 ago. 2021.

_____. Decreto nº 9.489, de 30 de agosto de 2018. Regulamenta, no âmbito da União, a Lei nº 13.675, de 11 de junho de 2018, para estabelecer normas, estrutura e procedimentos para a execução da Política Nacional de Segurança Pública e Defesa Social. **Diário Oficial da União**, Brasília, 31 ago. 2018c. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9489.htm. Acesso em: 04 ago. 2021.

_____. Decreto nº 10.882, de 03 de dezembro de 2021. Regulamenta o Tratado de Marraqueche para Facilitar o Acesso a Obras Publicadas às Pessoas Cegas, com Deficiência Visual ou com Outras Dificuldades para Ter Acesso ao Texto Impresso. **Diário Oficial da União**, Brasília, DF, 06 dez. 2021a. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Decreto/D10882.htm#:~:text=DECRETO%20N%C2%BA%2010.882%2C%20DE%203%20DE%20DEZEMBRO%20DE%202021&text=Regulamenta%20o%20Tratado%20de%20Marraqueche,Ter%20Acesso%20ao%20Texto%20Impresso. Acesso em: 04 ago. 2021.

_____. Câmara dos Deputados. **Projeto de Lei nº 9.736**, de 07 de março de 2018. Acrescenta dispositivo à Lei nº 7.210, de 11 de julho de 1984, para incluir a previsão de identificação por reconhecimento facial. Brasília, DF, 2018d. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2169011. Acesso em: 04 ago. 2021.

_____. Câmara dos Deputados. **Projeto de Lei nº 4.612**, de 21 de agosto de 2019. Dispõe sobre o desenvolvimento, aplicação e uso de tecnologias de reconhecimento facial e emocional, bem como outras tecnologias digitais voltadas à identificação de indivíduos e à predição ou análise de comportamentos. Brasília, DF, 2019b. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2216455. Acesso em: 04 ago. 2021.

_____. Decreto nº 9.854, de 25 de junho de 2019. Institui o Plano Nacional de Internet das Coisa e dispões sobre a Câmara de gestão e acompanhamento dos sistemas de comunicação máquina a máquina e internet das coisas. **Diário Oficial da União**, Brasília, DF, 25 jun. 2019c. Disponível em: http:// http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9854.htm. Acesso em: 04 ago. 2021.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. Secretaria de Empreendedorismo e Inovação. **Estratégia Brasileira de Inteligência Artificial – EBIA**. [s.l.], 2021b. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ia_estrategia_documento_referencia_4-979_2021.pdf. Acesso em: 05 nov. 2021.

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

_____. Ministério da Segurança Pública. **Plano Nacional de Segurança Pública e Defesa Social 2018-2028**. 2018f. 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.

_____. Ministério de Segurança Pública. **Plano Nacional de Segurança 2000**. Disponível em: https://cispregional.mpba.mp.br. Acesso em: 20 dez. 2020.

_____. Senado Federal. **Brasil poderá ter marco regulatória para a inteligência artificial**. Brasília, DF, 30 mar. 2022a. Disponível em: https://www12.senado.leg.br/noticias/materias/2022/03/30/brasil-podera-ter-marco-regulatorio-para-a-inteligencia-artificial. Acesso em: 10 abr. 2022.

_____. Senado Federal. **Projeto de Lei nº 5.762/2019**. LGPD Penal – exposição de motivos. Brasília, DF, 2019c. Disponível em: https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf. Acesso em: 11 fev. 2022.

_____. Senado Federal. Comissões do Senado. **Painel 7 - Inteligência Artificial e riscos:** vieses e discriminação. Brasília, DF, 2022b. Disponível em: https://legis.senado.leg.br/comissoes/reuniao?0&reuniao=10725&codcol=2504. Acesso em: 10 jun 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.

_____. Superior Tribunal de Justiça. Habeas Corpus. Pedido liminar. **Habeas Corpus nº 631298 BA 2020/0325153-1**, **do Governador do Estado da Bahia, Secretário de Segurança Pública do Estado da Bahia e Comandante da Polícia Militar do Estado da Bahia**. Brasília, 03 dez. 2020.

_____. Tribunal de Justiça da Bahia. Mandado de Segurança Cível. **Processo nº 8000691-28.2021.8.05.0000**. Impetrante: Alain Amorim. Impetrados: Secretário de Segurança Pública do Estado da Bahia, Comandante Geral da Polícia Militar do Estado da Bahia, Governador do Estado da Bahia. Relator: Des. Maurício Kertzman Szporer. Salvador, 2021c. Disponível em: https://jurisprudencia.tjba.jus.br/. Acesso em: 04 abr. 2022.

BRASIL. Tribunal de Justiça da Bahia. **Recurso de Apelação de sentença absolutória. Processo nº 000502162012.8.05.0191**. Apelante: Ministério Público da Bahia. Relatora: Des. Nágila Maria Sales Brito. Salvador, 14 abr. 2014b. Disponível em: https://jurisprudencia.tjba.jus.br/. Acesso em: 04 abr. 2022.

_____. Tribunal de Justiça da Bahia. **Habeas Corpus Criminal nº 8006504-70.2020.8.05.0000.** Órgão Julgador: Primeira Câmara Criminal 1ª Turma. Paciente: Leonardo Vinicius Bastos Carneiro Dantas e outros. Impetrado: Juiz de Direito de Senhor do Bonfim. Relator Des. Aldenilson Barbosa dos Santos. Salvador, 26 nov. 2021d. Disponível em: https://jurisprudencia.tjba.jus.br/. Acesso em: 04 abr. 2022.

_____. Gov.br. Disponível em: www.gov.br. Acesso em: 04 nov. 2021.

BUCCI, M. P. D. **Direito Administrativo e Políticas Públicas**. São Paulo: Saraiva, 2006.

BUOLAMWINI, J. A.; GEBRU, T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. 2018. **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.

_____. **Gender Shades**. 2020. Meet Media Lab. Disponível em: http://gendershades.org/. Acesso em: 01 set. 2020.

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

CASTELLS, M. **A Galáxia Internet:** reflexões sobre internet, negócios e sociedade. [s.l.: s.n.], 2004.

_____. **A Sociedade em rede**. Tradução: Rosineide Venâncio Majer; Atualiz. 6. ed.: Jussara Simões. São Paulo: Paz e Terra, 1999. (A era da informação: economia, sociedade e cultura, v. 1). Disponível em: https://globalizacaoeintegracaoregionalufabc.files.wordpress.com/2014/10/castells-m-a-sociedade-em-rede.pdf. Acesso em: 04 maio 2020.

CELLARD, A. A análise documental. *In*: POUPART, J. *et al*. **A pesquisa qualitativa**: enfoques epistemológicos e metodológicos. Petrópolis: Vozes, 2008.

CENTRO DE ESTUDOS DE SEGURANÇA E CIDADANIA. **O Panóptico:** monitor do reconhecimento facial no Brasil. Rio de Janeiro, 2019. Disponível em: https://cesecseguranca.com.br/?s=panoptico. Acesso em: 08 dez. 2020.

CHAER, G.; DINIZ, R. R. P.; RIBEIRO, E. A. A técnica do questionário na pesquisa educacional. **Evidência**, Araxá, v. 7, n. 7, p. 251-266, 2011. Disponível em: http://www.educadores.diaadia.pr.gov.br/arquivos/File/maio2013/sociologia_artigos/pesqusia_social.pdf. Acesso em: 01 dez. 2021.

CNJ. **Mandados de prisão pendentes de cumprimento de foragidos e procurados no Estado da Bahia**. Disponível em: https://portalbnmp.cnj.jus.br/#/estatisticas. Acesso em: 14 jul. 2022.

CNJ. **Portal do BNMP**. Disponível em: https://portalbnmp.cnj.jus.br/#/estatisticas. Acesso em: 16 jun. 2022.

CODED BIAS. Direção: Shalini Kantayya. 26 jan. 2020. Documentário disponível na Netflix. Acesso em: 04 abr. 2021.

CONGRESSO UFBA 75 ANOS. **Racismo algorítmico, reconhecimento facial e Segurança pública**: o cenário brasileiro. 2021. Disponível em: https://www.youtube.com/watch?v=j3JW_icY1kE&t=3375s. Acesso em: 07 dez. 2021.

COSTA, A. T.; LIMA, R. S. **Segurança pública:** crime, polícia e justiça no Brasil. São Paulo: Contexto, 2014.

COSTA JÚNIOR, P. J. **O direito de estar só:** tutela penal da intimidade. São Paulo: RT, 1995.

COSTA, R. da. **Sociedade do Controle**. São Paulo, 2004. Disponível em: https://www.scielo.br/j/spp/a/ZrkVhBTNkzkJr9jVw6TygVC/?lang=pt. Acesso em: 02 fev. 2022.

COSTA, R. S.; OLIVEIRA, S. R. O uso de tecnologias de reconhecimento facial em sistemas de vigilância e suas implicações no direito à privacidade. **Revista de Direito, Governança e Novas Tecnologias**, Belém, v. 5, n. 2. P. 1-21, jul./dez. 2019.

OLIVEIRA, L. V. *et al*. Aspectos ético-jurídicos e técnicos do emprego de reconhecimento facial na segurança pública do Brasil. **Revista Tecnologia e Sociedade**, Curitiba, v. 18, n. 50, p. 114-135, jan./mar. 2022. ISSN: 1984-3526. Disponível em: https://periodicos.utfpr.edu.br/rts/article/viewFile/12968/8625. Acesso em: 04 mar. 2022.

DATA PRIVACY BRASIL RESEARCH. **Defendendo o Brasil do Tecnoautoritarismo**. São Paulo, [2020?]. Disponível em: https://www.dataprivacybr.org/projeto/defendend_o_brasil_do_tecnoautoritarismo/2021. Acesso em: 28 jan. 2022.

DAWLER, T. Inteligência artificial, tecnologias informacionais e seus possíveis impactos sobre as Ciências Sociais. Dossiê/Metodologias Informacionais. **Sociologias,** n. 5, 2021. Disponível em: https://www.scielo.br/j/soc/a/CQffRYmfngbLzYQ9s6Mgr6m. Acesso em: 28 jan. 2022.

DECLARAÇÃO universal de direitos humanos. Adotada e proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III), 10 dez. 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 05 jan. 2021.

DISTRITO FEDERAL. Decreto nº 6.782, de 20 de maio de 2020. Altera a Lei nº 5.691, 2 de agosto de 2016, que dispõe sobre a regulamentação da prestação do Serviço de Transporte Individual Privado de Passageiros Baseado em Tecnologia de Comunicação em Rede no Distrito Federal e dá outras providências. **Diário Oficial do Estado**, Brasília, DF, 21 maio 2020. Disponível em: https://www.legisweb.com.br/legislacao/?id=395747. Acesso em: 04/08/2021.

DONDA, D. **Guia Prático de Implementação da LGPD**. São Paulo: Labrador, 2020.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658. Acesso em: 02 out. 2019.

_____. **Da privacidade à proteção dos dados pessoais**. Rio de Janeiro: Renovar, 2006.

DUARTE, D. E. Câmeras corporais e a ação policial: As condições de emergência e os impactos dos dispositivos de controle em São Paulo. **NEV**, São Paulo, c2022. 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.

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

EUA. **Ordinance 107-19**. Administrative Code - Acquisition of Surveillance Technology. San Francisco, jun. 04, 2019. Disponível em: https://sfbos.org/sites/default/files/o0107-19.pdf. Acesso em: 05 jan. 2021.

EUROPA. **EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces and some other uses of AI that can lead to unfair discrimination**. Bruxelas, 21 jun. 2021a. Disponível em: https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition_en. Acesso em: 11 fev. 2022.

_____. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. **Jornal Oficial da União Europeia L 119**, p. 89, 05 abr. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=HR. Acesso em: 14 nov. 2021.

_____. European Data Protection Board. **Guidelines 3/2019 on processing of personal data through video devices**. [s.l.], jan. 30 2020. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en. Acesso em: 14 nov. 2021.

_____. Parlamento Europeu. **A Inteligência Artificial na era digital**. Resolução do Parlamento Europeu, de 3 de maio de 2022, sobre a inteligência artificial na era digital. Estrasburgo, 3 maio 2022. (2020/2266(INI)). Disponível em:

https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_PT.html. Acesso em: 15 jun. 2022.

EUROPA. **Proposal for a Regulation of the Europeans Parliament and of the Concucil Laying down harmonized rules on artificla intelligende (Artificial Intelligence Act) anda amending certain union legislative acts**. 2021b. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 Acesso em: 30 nov. 2021.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **Facial recognition technology**: fundamental rights considerations in the context of law enforcement. Vienna, 27 nov. 2019. Disponível em: https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law. Acesso em: 14 nov. 2021.

EUROSTAT. **Estatística sobre criminalidade**. 2018. Disponível em: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Archive:Estat%C3%ADsticas_sobre_a_criminalidade&oldid=506918. Acesso em: 20/07/2022.

FALCAO, C. Rui Costa está transformando a Bahia em um laboratório de vigilância com reconhecimento facial. 20 set. 2021. 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.

FAROL NEWS. **1200 câmeras inteligentes passam a reforçar a segurança pública na Bahia**. Salvador, 14 jun. 2022. Disponível em: https://farolnews.com.br/mais-1200-cameras-inteligentes-passam-a-reforcar-a-seguranca-publica-na-bahia/. Acesso em: 15 jun. 2022.

FERRAZ JÚNIOR, T. S. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito**, São Paulo, Universidade de São Paulo, v. 88, p. 439-459, 1993.

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

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Nota Técnica** - Política de Ciência, Tecnologia e Inovação para a Segurança Pública. São Paulo, 2021. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2021/07/politica-de-ciencia-tecnologia-e-inovacao-para-seguranca-publica.pdf. Acesso em: 20 abr. 2022.

_____. **Reconhecimento Facial e Segurança Pública**. 08 dez [202-]. Disponível em: https://www.youtube.com/watch?v=TpR9Ke2YzZ4. Acesso em: 16 jun. 2022.

_____. **7º Anuário Brasileiro de Segurança Pública 2013.** Disponível em: https://forumseguranca.org.br/storage/7_anuario_2013-corrigido.pdf. Acesso em: 12 fev. 2022.

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

FOUCAULT, M. **Microfísica do Poder.** 2011 Disponível em: http://www.foucault.ileel.ufu.br/foucault/textos/microfisica-do-poder. Acesso em: 02 jan. 2021.

FRANCISCO, P. A. P.; HUREL, L. M.; RIELLI, M. M. Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais. **Revista Tecnologia e Sociedade**, v. 18, n. 50, p. 114-135, 2022.

FYLE, D. S.; DOLAN, K.; HUNT, V.; PRINCE, S. **Diversity wins**: how inclusion matters. Maio. 2019. Disponível em: https://www.mckinsey.com/featured-insights/diversity-and-inclusion/diversity-wins-how-inclusion-matters. Acesso em: 30 abr. 2021.

FRANQUEIRA, B. D.; HARTMANN, I. A.; SILVA, L. A. da. O que os olhos não veem, as câmeras monitoram: reconhecimento facial para a segurança pública e regulação na América Latina. **Revista Digital de Direito Administrativo**, Ribeirão Preto, SP, v. 8, n. 1, p. 171-204, 2021. Disponível em: https://www.revistas.usp.br/rdda/article/view/173903/168395. Acesso em: 22 jan. 2021.

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

G1 BAHIA. **Inaugurado centro que vai controlar ações de segurança da Copa na BA**. Salvador, 13 jun. 2013. Disponível em: https://g1.globo.com/bahia/noticia/2013/06/inaugurado-centro-que-vai-controlar-acoes-de-seguranca-da-copa-na-ba.html. Acesso em: 08 jun. 2021.

_____. **Sistema de reconhecimento facial é testado no embarque do aeroporto de Salvador; cidade é 1ª capital do NE a ter esse serviço**. Salvador, 17 dez. 2020. Disponível em: https://g1.globo.com/ba/bahia/noticia/2020/12/17/sistema-de-reconhecimento-facial-e-testado-no-embarque-de-passageiros-no-aeroporto-de-salvador.ghtml. Acesso em: 03 maio 2021.

_____. **Uma em cada 5 pessoais na Bahia se declara presta, aponta IBGE.** Salvador, 22 maio 2019. Disponível em: https://g1.globo.com/ba/bahia/noticia/2019/05/22/uma-em-cada-5-pessoas-na-bahia-se-declara-preta-aponta-ibge.ghtml. Acesso em: 25 ago. 2020.

G1. **Câmeras de reconhecimento facial ajudam a polícia a encontrar criminosos**. [s. l.], 10 mar. 2019a. Disponível em: https://g1.globo.com/fantastico/noticia/2019/03/10/cameras-de-reconhecimento-facial-ajudam-a-policia-a-encontrar-criminosos.ghtml. Acesso em: 04 maio 2021.

_____. **Huawei testou sistema de reconhecimento facial que emitia alerta de acordo com etnia, diz jornal**. Rio de Janeiro, 15 dez. 2020. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/12/15/huawei-testou-sistema-de-reconhecimento-facial-que-emitia-alerta-de-acordo-com-etnia-diz-jornal.ghtml. 2020. Acesso em: 06 fev. 2022.

G1. **Monitor da Violência:** assassinatos caem em 2019, mas letalidade policial aumenta; nº de presos provisórios volta a crescer. 16 dez. 2019b. 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.

G1 DISTRITO FEDERAL. **Lei regulamenta uso da tecnologia de reconhecimento facial em áreas públicas do DF**. Brasília, 12 nov. 2020. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2020/11/12/lei-regulamenta-uso-da-tecnologia-de-reconhecimento-facial-em-areas-publicas-do-df.ghtml. Acesso em: 10 fev. 2022.

G1 RIO. **Policiais vão começar a usar câmera nos uniformes no dia 16 de maio, anuncia governo**. Rio de Janeiro, 27 abr. 2022. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2022/04/27/policias-vao-comecar-a-usar-cameras-nos-uniformes-no-dia-16-de-maio-anuncia-governo.ghtml. Acesso em: 30 abr. 2022.

_____. **Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano**. Rio de Janeiro, 17 jul. 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml. Acesso em: 26 nov. 2022.

GIL, C. A. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GODOY, A. S. Pesquisa Qualitativa: tipos fundamentais. **Revista de Administração de Empresas**, São Paulo, v. 26, n. 2, 1995.

GÓIS, A. C. Congresso do EUA visa regular prisão por reconhecimento facial. 16 jul. 2021. Disponível em: https://www.tecmundo.com.br/seguranca/221235-congresso-eua-visa-regular-prisao-reconhecimento-facial.htm. Acesso em: 09 fev. 2022.

GOMES, H. S. **Por que uma das maiores cidades dos EUA baniu o reconhecimento facial?** São Paulo, 16 maio 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/05/16/por-que-uma-das-maiores-cidades-dos-eua-baniu-o-reconhecimento-facial.htm. Acesso em: 01 nov. 2020.

GONÇALVES, T.; MACHADO, C. N.; VARELLA, M. D. Os desafios da Administração Pública na disponibilização de dados sensíveis. **Revista Direito FGV**, v. 14, n. 2, São Paulo, maio-ago. 2018.

GOULART, B. B.; TIMM, L. B. "Viés" do algoritmo: computadores induzem decisões humanas erradas? 17 dez. 2020. Disponível em: https://www.migalhas.com.br/depeso/338056/vies--do-algoritmo--computadores-induzem-decisoes-humanas-erradas. Acesso em: 02 fev. 2022.

GRECO, Rogério. **Direitos humanos, sistema prisional e alternativas à privação de liberdade.** São Paulo: Saraiva, 2011.

GROTHER, P.; NGAN, M.; HANAOKA, K. **Face Recognition Vendor Test (FRVTV). Part 3: Demographic Effects**. National Institute Stardards and Tecnologys; USA Departament of Commerce: [s.l.], dec. 2019. Disponível em: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf. Acesso em: 03 fev. 2022.

HAN, B. C. **No enxame:** perspectiva do digital. Tradução Lucas Machado. Petrópolis, RJ: Vozes, 2018.

HIRATA, A. Direito à privacidade. Tomo Direito Administrativo e Constitucional, Edição 1, Abril de 2017. *In*: ENCICLOPÉDIA Jurídica da PUCSP, São Paulo, [2017?]. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade. Acesso em: 03 dez. 2021.

HONG, S. H. **Technologies of speculation**: the limits of Knowledge min a Dta-Driven Society. Nova York, NYU Press, 2020.

HORA, A. C. das N. S. da. **Ética em IA:** investigando o racismo algorítmico no reconhecimento facial. 2022. Dissertação (Mestrado)- Pontifícia Universidade de Católica do Rio de Janeiro, Rio de Janeiro, 2022. Disponível em: https://www.maxwell.vrac.puc-rio.br/colecao.php?strSecao=resultado&nrSeq=57522@1. Acesso em: 03 maio 2022.

HUAWEI. **Information Corporate**. [s.l.], c2022. Disponível em: https://www.huawei.com/br/corporate-information. Acesso em: 10 jun. 2021.

IBM. **Carta de Banimento da Tecnologia endereçada ao Presidente dos Estados Unidos Jon Biden**. [s.l.], 9 nov. 2020. Disponível em: https://www.ibm.com/blogs/policy/ibm-ceo-letter-to-president-elect-biden/. Acesso em: 09 dez. 2021.

ICHI.PRO. **O reconhecimento facial é a mais nova arma da política contra os manifestantes**. [s.l.], 2020. Disponível em: https://ichi.pro/pt/o-reconhecimento-facial-e-a-mais-nova-arma-da-policia-contra-os-manifestantes-219530644047595. Acesso em: 04 out. 2021.

IBGE. **Pesquisa Nacional por Amostra de Domicílio Contínua Anual - PNAD:** microdados 2018. Rio de janeiro: IBGE, 2018. 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.

INSTITUTO IGARAPÉ. **Desde 2011 vem sendo utilizado o reconhecimento facial no Brasil**. São Paulo, [entre 2019 e 2021]. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 05 fev. 2022.

INSTITUTO IGARAPÉ. [portal institucional]. Rio de Janeiro, jun. 2020. ISSN 2359-0998. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf. Acesso em: 04 mar. 2022.

ITS. **Resumo detalhado dos Planos Estratégicos de desenvolvimento de Inteligência Artificial**. Rio de Janeiro, mar. 2020. Disponível em: https://itsrio.org/wp-content/uploads/2020/03/RelatorioAI.pdf. Acesso em: 28 jan. 2022.

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

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

KAUFMAN, D. Deep learning: a Inteligência Artificial que domina a vida do século XXI. **Revista Digital de Tecnologias Cognitivas**, São Paulo, n. 17, p. 17-30, jan.-jun. 2018a. ISSN: 1984-3585. Disponível em: https://www.pucsp.br/pos/tidd/teccogs/edicao_completa/teccogs_cognicao_informacao-edicao_17-2018-completa.pdf. Acesso em: 08 set, 2020.

KAUFMAN, D. Entrevista com Davi Geiger. **Revista Digital de Tecnologias Cognitivas**, São Paulo, n. 17, p. 10-15, jan.-jun. 2018b. Disponível em: https://www.pucsp.br/pos/tidd/teccogs/edicao_completa/teccogs_cognicao_informacao-edicao_17-2018-completa.pdf. Acesso em: 08 set. 2020.

KAUFMAN, D. O protagonismo dos algoritmos da Inteligência Artificial: observações sobre a sociedade de dados. **Revista Digital de Tecnologias Cognitivas**, São Paulo, n. 17, p. 44-58, jan.-jun. 2018c. Disponível em: https://www.pucsp.br/pos/tidd/teccogs/edicao_completa/teccogs_cognicao_informacao-edicao_17-2018-completa.pdf. Acesso em: 08 set. 2020.

KOERNER, A. Capitalismo e vigilância digital na sociedade democrática. **Rev. Bras. Ci. Soc**., v. 36, n. 105, 2021. Disponível em: https://www.scielo.br/j/rbcsoc/a/3RSTj7mCYh6YcHRnM8QZcYD/. Acesso em: 03 abr. 2021

LABORATORIO DE ANÁLISE DE VIOLÊNCIA. **Mapeamento do programa de prevenção a homicídio na América Latina e Caribe**. Rio de Janeiro: Universidade Federal do Rio de Janeiro, 2016. Disponível em: http://www.lav.uerj.br/relat2016.html. Acesso em: 04 fev. 2022.

LAPIN. **Nota Técnica sobre a Lei Distrital nº 6.712/2020 DF**. 10 Recomendações para o uso do reconhecimento facial para a segurança pública no DF. [s.l.], 22 fev. 2021. Disponível em: https://lapin.org.br/2021/02/22/nota-tecnica-lei-distrital-6712-2020-df/#:~:text=A%20Lei%20Distrital%20n%C2%BA%206.712%2F2020%20foi%20editada%20num%20momento,no%20centro%20do%20debate%20p%C3%BAblico. Acesso em: 10 fev. 2022.

LEE, D. San Francisco is the first US city to ban facial recognition. may 2019. Disponível em: https://www.bbc.com/news/technology-48276660. Acesso em: 01 set. 2020.

LEMOS, E. et al. Comentários ao anteprojeto de Lei de proteção de dados para a Segurança Pública: Tecnologia de Reconhecimento Facial. mar. 2021. Disponível em:

https://itsrio.org/wp-content/uploads/2021/04/UK-Comentarios_LGPDPenal.pdf. Acesso em: 10 out. 2022.

LEVY, P. **Cibercultura**. São Paulo: Editora 34, 1999.

_____. **Inteligencia Colectiva**: por uma antropologia del ciberspacio. Trad. do francês por Felipe Mártinez Álvarez. [s.l.: s.n.], 2011. Disponível em: https://drive.google.com/drive/folders/0B-YLV8egGwSuUm9yRldCbWgzbVU. Acesso em: 10 dez. 2020.

LIMA, D. Racismo Algoritmo quando o preconceito chega a internet. **Humanista**, Porto Alegre, 17 nov. 2020. Disponível em: https://www.ufrgs.br/humanista/2020/11/17/racismo-algoritmico-quando-o-preconceito-chega-pela-internet/. Acesso em: 04 maio 2021.

LIMA, E. K. Agência de proteção de dados pede banimento do reconhecimento facial na Europa. 26 abr. 2021. Disponível em: https://olhardigital.com.br/2021/04/26/seguranca/agencia-de-protecao-de-dados-pede-banimento-do-reconhecimento-facial-na-europa/. Acesso em: 12 dez. 2021.

LIMA, G. D. de; OLIVEIRA, N. F. de; COSTA, S. T. da S. Gestão da Segurança Pública no Brasil: a utilização da Tecnologia a favor da sociedade. **GETEC**, Monte Carmelo, MG, v. 10, n. 25, p. 101-118, 2021. Disponível em: https://revistas.fucamp.edu.br/index.php/getec/issue/view/142. Acesso em: 04 fev. 2022.

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

LOPES. R. S. As TICs e a "Nova Economia": Para além do determinismo Tecnológico. **Ciência e Cultura**, São Paulo, v. 60, n. 1, 2008. Disponível em: http://cienciaecultura.bvs.br/scielo.php?script=sci_arttext&pid=S0009-67252008000100012. Acesso em: 03 abr. 2021.

MAGALHÃES, R.; VENDRAMINI. A. Os impactos da Quarta Revolução Industrial. **GVExecutivo**, v. 17, n. 1, jan.-fev. 2018. Disponível em: https://pesquisa-eaesp.fgv.br/sites/gvpesquisa.fgv.br/files/arquivos/annelisegv_v17n1_ar3.pdf. Acesso em: 20 dez. 2021.

MALDONADO, V. N.; BLUM, R. O. (coord.). **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2019.

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

MCCARTHY, J. **What is artificial intelligence?** Stanford, CA: Stanford University, 2007. Disponível em: http://www-formal.stanford.edu/jmc/whatisai.pdf. Acesso em: 30 ago. 2021.

MENEZES, P. Fases da Revolução Industrial: características e mudanças na produção. c2022. Disponível em: https://www.diferenca.com/revolucao-industrial/. Acesso em: 03 dez. 2022.

MELO, J. S. S.; NEVES, T. A; OLIVEIRA NETO, C. Amon: Controle de acesso do jurisdicionado no TJDFT, a partir de técnicas de reconhecimento facial. **Revista Eletrônica do CNJ**, v. 5, n. 1, p. 129-140, jan.-jun. 2021. ISSN 2525-4502. Disponível em: https://www.cnj.jus.br/ojs/index.php/revista-cnj/issue/view/7. Acesso em: 29 jan. 2022.

SMITH, B. Reconhecimento Facial é hora de agir. 2018. Disponível em: www.newsmicrosoft.com. Acesso em: 03 abr. 2020.

MIGLIANO, S. Hikvision and Dahua Surveillance Camera Networks Investigation. **Hikvision and Dahua Surveillance Camera Networks Data Sheet**, [s.l.], 2021. Disponível em: https://docs.google.com/spreadsheets/d/1vjSkIIORhZjlAVM500ZtzLpc0BBcHVJ0KJjK85GvXLQ/edit#gid=1358637582. Acesso em: 29 jan. 2022.

MINAS GERAIS. Assembleia Legislativa. Entenda: Informações gerais. 2022. Disponível em: https://politicaspublicas.almg.gov.br/temas/seguranca_publica/entenda/informacoes_gerais.html?tagNivel1=302&tagAtual=302. Acesso em: 05 ago. 2022.

MOREIRA, P. P. Tratamento e Uso compartilhado de dados pessoais pela administração pública na execução de políticas públicas. *In:* POZZO, A. N. D.; MARTINS, R. M. (coord.). **LGPD e Administração Pública**. São Paulo: Revista dos Tribunais, 2020. p. 275-292.

MOZUR, P. Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras. **The New York Times**, New York, 8 jul. 2018. Disponível em: https://scholar.harvard.edu/people_analytics/publications/inside-chinas-dystopian-dreams-ai-shame-and-lots-cameras. Acesso em: 09 jan. 2022.

MULHOLAND, C., O tratamento de dados pessoais sensíveis. *In*: _____. (org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020.

MUNIZ, T. Reconhecimento Facial já prendeu 35 na Bahia; 3 mil são alvos da polícia. **Correio**, Salvador, 01 jun. 2019. Disponível em: https://www.correio24horas.com.br/noticia/nid/reconhecimento-facial-ja-prendeu-35-na-bahia-3-mil-sao-alvos-da-policia/. Acesso em: 04 set. 2021.

NEGRI, S. M. C. Á.; OLIVEIRA, S. R.; COSTA, R. S. 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, maio-jun. 2020.

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

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

NTECHLAB. **Plataforma de análise de vídeo multiobjetos**. c2022. Disponível em: https://ntechlab.com/pt_br/. Acesso em: 04 abr. 2022.

NUNES, F. T. et al. Um estudo sobre técnicas de biometria baseadas em padrões faciais e sua utilização. *In*: SPANHOL, J. F. (org.). **Tecnologia e Informação na Segurança Pública e Direitos Humanos**. v. 2. São Paulo: Editora Edgar Blucher, 2016.

OBSERVATÓRIO DE SEGURANÇA PÚBLICA. c2020. Disponível em: https://www.observatoriodeseguranca.org/a-seguranca-publica-no-brasil/#tab-polticasdeseguranapblica. Acesso em: 10 mar. 2022.

OLIVA, M. D.; SILVA, J. G. da. Discriminação algorítmica nas relações de consumo. **Migalhas**, [s.l.], 23 fev. 2021. Disponível em: https://www.migalhas.com.br/depeso/340680/discriminacao-algoritmica-nas-relacoes-de-consumo. Acesso em: 08 ago. 2021.

OLIVA, D. C. Em busca da Segurança: Tecnologias contra o medo. **Revista Discente do Programa de Pós-Graduação em Sociologia da Universidade do Paraná**, v. 03, n. 2, 2015. Disponível em: https://revistas.ufpr.br/sclplr/article/view/64765/37692. Acesso em: 12 abr. 2021.

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

OLIVEIRA, C. L. Um apanhado teórico-conceitual sobre a pesquisa qualitativa: tipos, técnicas e características. **Revista Travessia**, Cascavel: Unioeste, n. 4, 2009. Disponível em: https://e-revista.unioeste.br/index.php/travessias/article/view/3122. Acesso em: 08 jan. 2022.

OLIVEIRA. E. T. Bahia é a primeira no ranking de mortes violentas no Brasil. **Correio 24 horas**, Salvador, 22 abr. 2022. Disponível em: https://www.correio24horas.com.br/noticia/nid/bahia-e-primeira-no-ranking-de-mortes-violentas-no-brasil/. Acesso em: 08 maio 2022.

PAGNAN, R. No 1º mês de uso das câmeras 'grava-tudo', PM de SP atinge menor letalidade em 8 anos. **Folha de São Paulo**, São Paulo, 10 jul. 2021. Disponível em: https://www1.folha.uol.com.br/cotidiano/2021/07/no-1o-mes-de-uso-das-cameras-grava-tudo-pm-de-sp-atinge-menor-letalidade-em-8-anos.shtml. Acesso em: 02 maio 2022.

PALMA, A.; PACHECO, C. Entenda como funciona o reconhecimento facial que ajudou a prender mais de 100 na BA. **Correio 24 horas**, Salvador, 05 jan. 2020. 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.

PECK, P. P. **Direito Digital**. 6. ed. São Paulo: [s.n.], 2019.

_____. **Proteção de Dados Pessoais**: Comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Jur., 2020.

PEIXOTO, G. M. **A defesa dos direitos fundamentais pela jurisdição constitucional**. 2012. 251 p. Dissertação (Mestrado em Direito) – Faculdade de Direito da Universidade Federal da Bahia-UFBA, Salvador, 2012.

PEREIRA, A. C. S. et al. Inteligência artificial e direitos humanos: impactos e dilemas éticos atuais. **Homa Publica**: Revista Internacional de Direitos Humanos e Empresas, Juiz de Fora, MG, v. 4, n. 1, p. 1-18, jan./dez. 2020. Disponível em: https://periodicos.ufjf.br/index.php/HOMA/article/view/30504. Acesso em: 08 ago. 2021.

PINHEIRO, E. N. Políticas públicas e a proteção de dados pessoais: o uso da tecnologia de reconhecimento facial pela Secretaria de Segurança Pública do Estado da Bahia. *In*: SHEREMETIEFF, Adriana Henrichse al. (org.). **Visões Contemporâneas sobre Políticas Públicas** Rio de Janeiro: [s.n.], 2021. p. 562-579.

PINHEIRO, E. N.; FERRAZ, D. O uso da inteligência artificial na criação de profiling e o direito do titular dos dados na revisão automatizada. *In*: JESUS, D. M. de (org.). **Estudos multirreferenciados**. Salvador: Mente Aberta, 2021. p. 29-41, (Ciências Sociais Aplicadas, 5).

PIRES, A. B. S. et al. O uso do reconhecimento facial em Salvador. *In*: ALMEIDA, E. M.; ESTELLITA, H. (coord.). **Dados, privacidade e persecução penal**: cinco estudos. FGV, Data Privacy, 2021. p. 19-33. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/31784/Dados,%20privacidade%20e%20persecu%C3%A7%C3%A3o%20penal.pdf?sequence=1. Acesso em: 03 de maio de 2022.

PRESCOTT, R.; MARIANO, R. Salvador integra 1900 câmeras em sistema único de segurança. 25 out. 2018. Disponível em: https://www.convergenciadigital.com.br/Seguranca/Salvador-integra-1900-cameras-em-sistema-unico-de-seguranca-49299.html?UserActiveTemplate=mobile. Acesso em: 10 maio 2022.

POGREBINSCHI, T. Foucault, para além do poder disciplinar e do biopoder. **Lua Nova**: Revista de Cultura e Política, [s.l.], n. 63, p. 179-200, 2004. (Identidade e igualdades em conflito).

QUIVY, R.; CAMPENHOUDT, L. V. **Manual de Investigação em Ciências Sociais**. 2. ed. Lisboa: Gradiva, 1998. Disponível em: https://tecnologiamidiaeinteracao.files.wordpress.com/2018/09/quivy-manual-investigacao-novo.pdf. Acesso em: 03 jun. 2020.

R7. **Viaturas da PM são equipadas com câmeras e computador de bordo**. Salvador, 2014. Disponível em: https://noticias.r7.com/bahia/viaturas-da-pm-sao-equipadas-com-cameras-e-computador-de-bordo-28082015. Acesso em: 08 jun. 2021.

RIBEIRO, F. M. L. *et al*. Detecção de Pontos Fiduciais sobre a Face em Tempo Real. *In*: SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES, 30., Brasília, DF, 2012. **Anais** [...] Disponível em: www.biblioteca.sbrt.org.br. Acesso em: 29 jan. 2022.

ROSA, J. L. G. **Fundamentos da inteligência artificial.** Rio de Janeiro: LTC, 2011. Disponível em: http://walderson.com/2011-2/IA/FIA.pdf. Acesso em: 08 ago. 2021.

RODRIGUES, R. B. **Novas Tecnologias da Informação e da Comunicação**. Recife: IFPE, 2016. ISBN: 978-85-9450-008-3. Disponível em: https://www.ufsm.br/app/uploads/sites/413/2018/12/arte_tecnologias_informacao_comunicacao.pdf. Acesso em: 03 mar. 2022.

RODRIGUES, R. **Salvador e mais 77 municípios contarão com ampliação de serviço de reconhecimento facial e de placas.** Salvador: Secom, 27 jul. 2021. Disponível em: https://www.bahia.ba.gov.br/2021/07/noticias/salvador-e-mais-77-municipios-contarao-com-ampliacao-de-servico-de-reconhecimento-facial-e-de-placas/. Acesso em: 03 abr. 2022.

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

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

ROXIN, C. **Derecho Penal**. Parte General. Tomo I: fundamentos. La estructura de la teoría del delito. 2. ed. Madrid: Editorial Civitas, 1997.

RUSSEL, S.; NORVING, P. **Inteligência artificial**. Trad. Regina Célia Simille. Rio de Janeiro: Elsevier, 2013.

RUBACK, L.; AVILA, S.; CANTERO, L. **Vieses no aprendizado de máquina e suas implicações sociais**: um estudo de caso no reconhecimento facial. Porto Alegre, 2021. Disponível em: https://sol.sbc.org.br/index.php/wics/article/view/15967/15808. Acesso em: 04 nov. 2021.

SALVADOR (Município). Secretaria Municipal de Cultura e Turismo - SECULT. **PRODETUR Salvador - Licitações em andamento**. Disponível em: http://www.prodeturssa.salvador.ba.gov.br/index.php/licitacoes. Acesso em: 15 jun. 2022.

SANTOS, A. S.; LIMA, E. G. de; SOUZA, W. B. de **Tecnologia da Informação na Segurança Pública**: a necessidade de criação de uma base nacional de dados de registro de ocorrência e atendimentos de emergência. 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.

SÃO PAULO (Estado). Secretaria de Segurança Pública. **Retrato Falado**, São Paulo, 2021. Disponível em: https://www.ssp.sp.gov.br/fale/institucional/answers.aspx?t=12#:~:text=Para%20que%20serve%20um%20retrato,da%20idade%20ou%20reconstitui%C3%A7%C3%A3o%20facial. Acesso em: 03 abr. 2021.

SÁ-SILVA, J. R.; ALMEIDA, C. D. de; GUINDANI, J. F. Pesquisa documental: pistas teóricas e metodológicas. **Revista Brasileira de História & Ciências Sociais**, ano 1, n. 1, jul. 2009. ISSN: 2175-3423. Disponível em: www.rbhcs.com. Acesso em: 10 dez. 2021.

SCHALKOFF, J. R. **Artificial Intelligence Engine**. 19. Th. New York: MC-Graw-Hill, 1990.

SCHIER, A. C. R. **Princípio da universalidade.** Tomo Direito Administrativo e Constitucional, Edição 1, Abril de 2017. São Paulo, [2017?]. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/77/edicao-1/principio-da-universalidade#:~:text=O%20princ%C3%ADpio%20da%20universalidade%20ou,um%20car%C3%A1ter%20gen%C3%A9rico%20e%20universal. Acesso em: 10 maio 2022.

SCHNEIDER, C. B.; MIRANDA, P. F. M. Vigilância digital como instrumento de promoção de segurança pública. **Revista UEPG**, Ponta Grossa, n. 28, p. 1-14, 2020. Disponível em: https://www.revistas.uepg.br/index.php/sociais/article/view/14435/209209212734. Acesso em: 30 nov. 2021.

SCHWAB, K. **A quarta revolução industrial**. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016.

_____. **Aplicando a quarta revolução industrial**. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2019.

SERPRO. **Datavalid 2.0 chega a 99,9% de precisão no reconhecimento facial**. Brasília, DF, 2020. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2020/reconhecimento-facial-mais-preciso-com-datavalid. Acesso em: 10 abr. 2022.

SILBERG, J.; MANYIKA, J. Co**mo lidar com vieses na inteligência artificial (e nos seres humanos)**. 6 jun. 2019. Disponível em: https://www.mckinsey.com/featured-insights/artificial-intelligence/tackling-bias-in-artificial-intelligence-and-in-humans/pt-br. Acesso em: 01 fev. 2022.

SILVA, E. L.; MENEZES, E. M. **Metodologia de pesquisa e elaboração de dissertação**. 4. ed. Florianópolis: [s.n.], 2005.

SILVA JUNIOR, J. J. da. **Redes neurais profundas para reconhecimento facial no contexto de segurança pública**. 2020. 85 f. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Goiás, Goiânia, 2020. Disponível em: https://repositorio.bc.ufg.br/tede/handle/tede/10567. Acesso em: 02 fev. 2021.

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

SILVA NETO, V. J. ; BONACELLI, M. B. M; PACHECO, C. A. O sistema tecnológico digital: Inteligência artificial, computação em nuvem e Big Data. **Revista Brasileira de Inovação**, Campinas, SP, n. 19, p. 1-31, 2020. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/rbi/article/view/8658756. Acesso em: 14 fev. 2022.

SILVA, P. G. F. da. **Sorria você está sendo reconhecido**: o reconhecimento facial como violador de direito humanos? Rio de Janeiro, 26 ago. 2020. 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, R. L. da; SILVA, F. dos S. R. da. Reconhecimento facial e segurança pública: Os perigos do uso da tecnologia no sistema penal seletivo brasileiro. CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE, 5, 2019. **Anais** [...] Santa Maria, RS, set. 2019. Disponível em: https://www.ufsm.br/app/uploads/sites/563/2019/09/5.23.pdf. Acesso em: 06 set. 2020.

SILVA, S. P. da. Democracia, inteligência artificial e desafios regulatórios: Direitos, dilemas e poder nas sociedades datificadas. **E-legis**, Brasília, DF, n. 33, p. 226-248, set.-dez. 2020. ISSN: 2175.0688. Disponível em: https://e-legis.camara.leg.br/cefor/index.php/e-legis/article/view/600/802. Acesso em: 09 fev. 2021.

SILVA, T. *Linha do Tempo do Racismo Algorítmico*: casos, dados e reações. 2019a. Disponível em: http://https://tarciziosilva.com.br/blog/posts/racismo-algoritmico-linha-do-tempo. Acesso em: 03/04/2022.

_____. Racismo Algorítmico em Plataformas Digitais: microagressões e discriminação em código. *In*: _____. (org.). **Comunidades, algoritmos e ativismo digitais**: olhares afrodiaspóricos. São Paulo: Literarua, 2020a.

_____. **Racismo Algoritmo, entre a (des)inteligência artificial e a epistemologia da ignorância.** São Paulo, 23 nov. 2020b. Disponível em: https://www.select.art.br/racismo-algoritmico/. Acesso em: 04 fev. 2022.

_____. "Racismo algoritmo": pesquisador mostra como os algoritmos podem discriminar. 06 ago. 2019b. Disponível em: https://www.rfi.fr/br/brasil/20190806-racismo-algoritmico-pesquisador-mostra-como-os-algoritmos-podem-discriminar. Acesso em: 04 fev. 2022.

_____. **Reconhecimento facial deve ser banido**. Veja dez razões: Disponível em: https://tarciziosilva.com.br/blog/reconhecimento-facial-deve-ser-banido-aqui-estao-dez-razoes/. Acesso em: 02 fev. 2022.

_____. **Twitter**. 2022. Disponível em: https://twitter.com/tarciziosilva. Acesso em: 15 jan. 2022.

SILVA, M. R. **Visibilidade trans**. 2021. Instagram: @opanópticobr. Disponível em: https://www.instagram.com/p/CZPkQcilyKh/. Acesso em: 04 jun. 2022.

SILVEIRA, D. T.; CÓRDOVA, F. P. **A pesquisa científica**. *In:* GERHARDT, T. E.; SILVEIRA, D. T. Métodos de pesquisa. Porto Alegre: UFRGS, 2009. cap. 02, p. 31-42. Disponível em: http://www.ufrgs.br/cursopgdr/downloadsSerie/derad005.pdf . Acesso em: 15 fev. 2022.

SIMON, M. HP looking into claim webcams can’t seem black people.24 dec. 2009. Disponível em: https://edition.cnn.com/2009/TECH/12/22/hp.webcams/index.html. Acesso em: 03/02/2022.

SIQUEIRA, D. P.; LARA, F. C. P. Quarta Revolução Industrial, inteligência artificial e a proteção do homem no direito brasileiro. **Revista Meritum,** v. 15, n. 4. p. 300-311, 2020. Disponível em: https://eds.p.ebscohost.com/eds/detail/detail?vid=1&sid=825b5068-aa49-4c35-b34b-541aa4ecacd9%40redis&bdata=Jmxhbmc9cHQtYnImc2l0ZT1lZHMtbGl2ZQ%3d%3d#AN=152543197&db=foh. Acesso em: 04 jan. 2022.

SOLOVE, D. J. **Understanding Privacy**. Cambridge, Havard University Press, 2008.

_____. **Nothing to Hide**: The false Tradeoff between Privacy and Security. New Haven: Yale University Press, 2011a.

_____. Why Privacy Matters Even if you have ‘Nothing to Hide’. **The Chronicle of higher education,** 2011b.

SILVEIRA, D. T.; CÓRDOVA, F. P. Métodos de Pesquisa. *In*: GERHARDT, E.; SOUZA, A. C. de (org.). **Unidade 2**: a pesquisa científica. 1. ed. Porto Alegre: UFRGS, 2009.

SMITH, B.; BROWNE, C. A. **Armas e Ferramentas**: O futuro e o perigo da Era Digital. São Paulo: Alta Books, 2021.

SOARES, L. E. **Meu casaco de general**. Quinhentos dias no front da Segurança Pública do Rio de Janeiro. São Paulo: Cia. das Letras, 2000.

SOUZA, M. A. de. A Biometria e suas aplicações. **Revista Brasileira de Ciências Policiais**, Brasília, DF, v. 11, n. 2, p. 79-102, maio-ago. 2020. Disponível em: https://periodicos.pf.gov.br/index.php/RBCP/article/view/710. Acesso em: 15 jan. 2021.

TAKARASHI, T. (org.) **Sociedade da Informação no Brasil**. Livro Verde. Brasília: Ministério da Ciência e Tecnologia, 2000.

UNIVERSIDADE DE SÃO PAULO. Biometria facial, segurança pública e monitoramento urbano. 2021. Disponível em: https://www.youtube.com/watch?v=VlN13KvujWY&t=17s. Acesso em: 10 jan. 2022.

USHIKOSHI, M. Ada Lovelace e o primeiro algoritmo da história. São Paulo, 24 ago. [202-?]. Disponível em: https://www.laraiatech.com/blog/ada-lovelace-e-o-primeiro-algoritmo-da-historia#:~:text=Em%201843%2C%20Lovelace%20traduziu%20uma,computava%20os%20n%C3%BAmeros%20de%20Bernoulli. Acesso em: 12 jan. 2022

VALENTE, J. Tecnologias de reconhecimento facial são usadas em 37 cidades do país. São Paulo, 19 set. 2019. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2019-09/tecnologias-de-reconhecimento-facial-sao-usadas-em-37-cidades-no-pais. Acesso em: 05 set. 2020.

_____. Tecnologias de reconhecimento facial se popularizam e levantam debate. **Correio 24 horas**, Salvador, 22 jul. 2018. Disponível em: https://www.correio24horas.com.br/noticia/nid/tecnologias-de-reconhecimento-facial-se-popularizam-e-levantam-debate/. Acesso em: 06 set. 2020.

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

VIDAL, E. L. **Monitoramento Eletrônico: Aspectos Teóricos e Práticos**. 106 f. 2014. 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.

VICTORINO, M. Os benefícios do reconhecimento facial como aliado da segurança nas empresas. **Revista de Segurança Eletrônica**, c2017. Disponível em: https://revistasegurancaeletronica.com.br/os-beneficios-do-reconhecimento-facial-como-aliado-da-seguranca-nas-empresas/. Acesso em: 04 maio 2022.

VIEIRA, S. **Como elaborar um questionário.** São Paulo: Atlas, 2009.

VILHENA, M. I. R. **Modelo de risco de terreno:** Uma estratégia preditiva para a implementação de sistemas de videovigilância. 82 f. 2019. (Dissertação) Mestrado – Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa, 2019. Disponível em: https://comum.rcaap.pt/handle/10400.26/30325. Acesso em: 03 abr. 2022.

WARREN, S.; BRANDEIS, L. The right to privacy. **Harvard Law Review,** Cambridge, v. 4, n. 5, dec. 1890.

WERTHEIN, J. A Sociedade da Informação e seus desafios. **Ci. Inf.**, Brasília, v. 29, n. 2, p. 71-77, maio-ago. 2000. Disponível em: https://www.scielo.br/j/ci/a/rmmLFLLbYsjPrkNrbkrK7VF/?format=pdf&lang=pt. Acesso em: 02 fev. 2022.

WOLF SILVER. 1984 – George Orwell – Grandes Livros. Disponível em: https://www.youtube.com/watch?v=ZURVt5hTld4. Acesso em: 02 abr. 2022.

YIN, R. K. **Estudo de caso - planejamento e métodos**. 3. ed. Porto Alegre: Bookman, 2005.

ZUBOFF, S. Big Brother*:* capitalismo de vigilância e perspectivas para uma civilização de informação. *In*: BRUNO, F. et al. (org.). **Tecnologias da vigilância**: perspectivas da margem. Trad. H. M. C. et al. São Paulo: Boitempo, 2018. p. 17-68.

APÊNDICE A – QUESTIONÁRIO

Prezados Senhores (as),

Boa tarde,

Venho pela presente, na condição de Mestranda em Direito, Governança e Políticas Públicas pela Universidade Salvador – Unifacs, com base na Lei de Acesso à Informação – Lei nº 12.527/2011, requerer informações sobre as políticas públicas que se utilizam do reconhecimento facial, via inteligência artificial, pela Secretaria de Segurança Pública do Estado da Bahia, para realização de pesquisa acadêmica.

Dessa maneira, envio abaixo um Questionário contendo dez questões abertas sobre a temática acima mencionada:

1) Gostaria de explicações técnicas sobre a tecnologia de reconhecimento facial utilizada e desde quando foi implantada na Bahia?

2) Qual a empresa que fornece a tecnologia utilizada para o reconhecimento facial utilizada pela SSP-BA? Houve licitação para a contratação?

3) Quantas pessoas foram identificadas pelo sistema de reconhecimento facial de sua implantação até esta data?

4) Qual é a base de dados que é utilizada para aplicação do comparativo para o reconhecimento facial das pessoas?

5) Há casos de erros quanto a identificação do sistema de reconhecimento facial para segurança pública? Se sim, numericamente, qual o percentual de erros nas identificações?

6) Com que percentual de semelhança com uma pessoa que consta nos registros da SSP-BA poderá ser abordada para investigação?

7) Quantas pessoas foram abordadas pela polícia e apontado equívocos no reconhecimento facial desde a sua implantação?

8) A SSP-BA fez alguma consulta pública ou medidas de participação social antes da implementação do reconhecimento facial como política pública?

9) Como são armazenados os dados biométricos extraídos pelo reconhecimento facial pela SSP-BA? Quem tem acesso a essas informações e que classificação documental elas são armazenadas?

10) Há compartilhamento dos dados biométricos de reconhecimento facial coletados com outros órgãos do governo, empresas privadas ou demais entidades da administração pública direta ou indireta, ou ainda outras entidades e governos internacionais?